Neue Kriminalitätsformen

Diese sind auf der hier eingefügten Aussendung der Vorarlberger Krfiminalpolizei zu finden:

.LPD REPUBLIK ÖSTERREICH
LANDESPOLIZEIDIREKTION VORARLBERG

LANDESKRIMINALAMT
LKA AB06 (IT/B) Informationstechnologie/Beweismittel

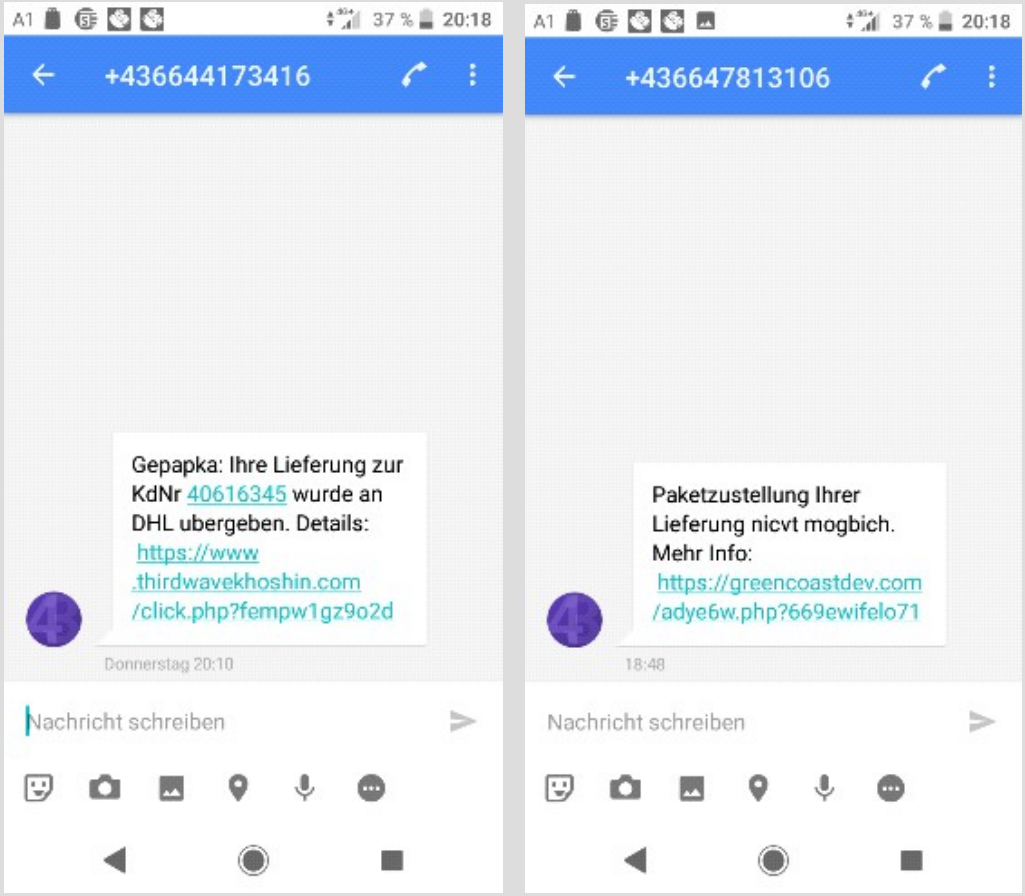
Neue Kriminalitätsformen
Informationen & Bearbeitungshilfen

Bregenz, am 25.05.2021
Aktualisiert 07.06.2021, KAUFMANN

Bearbeiter: Harald LONGHI ChefInsp

Massen-SMS
mit angeblichen Paket-Benachrichtigungen

Sachverhalt:
Seit dem Pfingstwochenende 2021 wurden österreichweit offensichtlich mehrere hunderttausend SMS mit Informationen zu einer angeblichen Paketlieferung samt Linkadresse versendet.



Die Links führen auf gehackte Webseiten, die miteinander verknüpft sind. Je nach verwendetem Gerät/Betriebssystem werden unterschiedliche Inhalte angezeigt.

- iOS – Phishingseite, Abofalle
- Android – Aufforderung zur Installation einer „App" aus einer externen Quelle; dabei handelt es sich um eine Version des Banking-/Kryptowährungstrojaners „FluBot/Cabassous".

Funktionsweise des Trojaners:
Sofern auf dem infizierten Androidgerät **eine Banking App installiert** ist, wird der Trojaner erst bei Aktivierung der Banking App aktiv und zieht Geld vom Bankkonto ab.

Falls **keine Banking App installiert** ist, scannt der Trojaner alle Apps und sucht nach Kryptowährungen und Zugangsdaten für soziale Netzwerke und Onlineshops. Außerdem versendet der Trojaner, wenn keine Banking App installiert ist, weitere Phishing-SMS an verschiedene Nummern im In- und Ausland, die keine Verbindung mit der Kontaktliste des Geschädigten aufweisen.

Polizeiliches Vorgehen:
In einer Besprechung am 31.05.2021 zwischen den zuständigen Bereichen im Bundeskriminalamt und den Landeskriminalämtern wurde die nachstehende Vorgehensweise bekanntgeben und auch im KLF veröffentlicht.

- Die Aktbearbeitung und -erledigung erfolgt im **eigenen** Wirkungsbereich. Die auf der jeweiligen Dienststelle angezeigten Sachverhalte können als eigene OZ in einer einzelnen GZ zusammengeführt werden.
- Das Bundeskriminalamt führt eine, aus dem SIMO generierte Excel-Liste, damit die Sachverhalte erforderlichenfalls im Nachhinein zusammengeführt werden können.
- Im Kurzsachverhalt ist neben der Beschreibung auch der im SMS **enthaltene Link** anzuführen.
- Jede OZ ist mit dem Schlagwort-Info „**Smishing – Paketversand**" zu versehen.

Einordnung der Delikte nach Vorgabe des .BK:

§ 126c StGB:	Opfer bekommt ein SMS mit Link (**kein Schaden)**
§ 148a StGB:	Opfer installiert die App (Trojaner!)
§ 241h StGB:	Opfer gibt auf einer Phishingseite Kreditkarten- oder Kontodaten bekannt
§ 119a StGB:	Opfer gibt andere Zugangsdatendaten (Amazon, Facebook udgl) bekannt

Daher gilt die mit der Staatsanwaltschaft Feldkirch am 07.06.2021 abgesprochene Vorgangsweise zur Bearbeitung auf den betroffenen Dienststellen:

- Wird der Empfang der SMS – **ohne Schaden -** „nur zur Kenntnis gebracht" – als „Wahrnehmung" des Betroffenen, dann ist eine GZ anzulegen und die jeweiligen Meldungsleger als Unter-OZ aufzunehmen / evident zu halten - mit einem AV.
- Wird der Empfang der SMS **angezeigt**, ist also aus der Meldung erkennbar, dass die Partei die Anzeige erstatten will, dann ist ein Bericht nach § 100 Abs3a StPO – als § 126c StGB zu erstatten.
- In den anderen Fällen, wenn also ein Trojaner installiert wurde, wenn Kreditkarten- oder Kontodaten bekannt gegeben wurden oder Zugangsdaten bekannt gegeben wurden, dann ist eine Anzeige nach §§ 148a, 241h oder 119a StGB mit Opferbefragung und einer Dokumentation zu erstatten.

Maßgebliche Daten der Vernehmung oder des Aktenvermerkes:
Im Zuge der Sachverhaltsaufnahme sind neben den grundsätzlichen Inhalten (7 W) folgende Informationen relevant:

- Betriebssystem und Version des Opferhandys
- Hat Opfer den Link angeklickt?
- Wurde die (schädliche) App auf das Handy geladen?
- Wurde das Opfer auf eine Phishingseite weitergeleitet? Wenn ja, welche?
- Wurden Daten auf einer Phishingseite eingegeben?
- Befinden sich Kryptowährungswallets oder Banking-Apps auf dem Handy?
- Welche Telefonnummer scheint als Absender auf?
- Link in Reinschrift schreiben – maßgeblich für weitere Ermittlungen
- Finanzieller Schaden?

- Wie entstanden? Abbuchungen oder Telefonrechnung?
- Bei Abbuchungen, wohin gingen die Zahlungen? (Empfänger, IBAN)
- Wie viele SMS wurden automatisch über die Schadsoftware versendet?

Informationen für die Opfer:

- Nach der Installation der „App" ist das Android-Gerät als unsicher zu betrachten!
- Der Trojaner kann laut bisherigen Erkenntnissen im „abgesicherten Modus" entfernt werden – Anleitung im KLF
- Wer ganz sicher sein will, sollte das Gerät auf Werkseinstellung zurücksetzen (Datenverlust!)
- Keine Apps aus externen Quellen installieren!
- Kontaktaufnahme mit dem Telefonanbieter und dem Konsumentenschutz – eventuell wird kulanzhalber auf die entstandenen SMS-Kosten verzichtet
- Bankkonten, Kreditkarten und Wallets über ein sicheres Gerät kontrollieren.