heise Security

Voice-Phishing: Betrüger setzen auf raffinierte Vishing-Masche

11.07.2023 09:42 Uhr Dirk Knop

(Bild: Shutterstock/New Africa)

Betrüger erklimmen beim Voice-Phishing (Vishing) das nächste Level: Sie leiten etwa gezielt Anrufe um, um betrügerische Abzocke zu verschleiern.

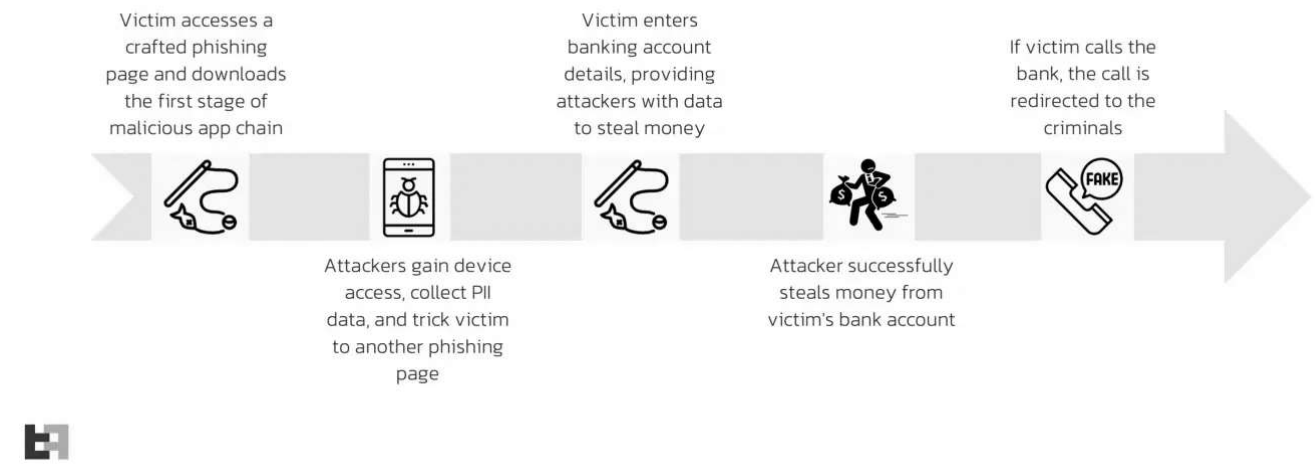
Das Smartphone klingelt, dran ist ein vermeintlicher Bankberater: "Hier spricht das Sicherheits-Team Ihrer Bank – die Nachrichten, die Sie erhalten, sind kein Problem, machen Sie sich keine Sorgen!" Solch ein Anruf ist Teil einer jetzt aufgedeckten, besonders raffinierten Voice-Phishing-Kampagne mit dem Codenamen "Letscall". Bei Voice-Phishing, kurz Vishing genannt, handelt es sich um eine perfide Betrugsmasche.

IT-Forscher von Threatfabric haben eine fortschrittliche, professionelle und komplexe Vishing-Masche aufgedeckt, die derzeit in Südkorea zu beobachten ist. Sie sei aber problemlos auch in Europa umzusetzen, erklären die **IT-Analysten in ihrem Blog-Beitrag [1]**.

Vishing-Masche: Kreditaufnahme im Namen der Opfer

Die Angreifer locken die potenziellen Opfer auf zunächst eine gut aufgemachte Phishing-Seite, die dem Google Play Store stark ähnelt. Von dort laden Opfer die erste Stufe der bösartigen Apps herunter. Die fragt die nötigen Berechtigungen an, öffnet die eigentliche Phishing-Seite und lädt die zweite Malware vom Control-Server herunter. Die zweite Stufe sammelt Daten ein, schleust sie an die Cyberkriminellen aus und bindet infizierte Geräte in das Peer-to-Peer-VoIP-Netz ein.

Letscall setzt dabei auf WebRTC-Technik, um VoIP-Verkehr umzuleiten und die Opfer mit den Call-Center-Mitarbeitern zu verbinden. Eine weitere, dritte Malware ergänzt die zweite Schadcode-Datei um Anruf-Funktionen, die die Betrüger für die Rufumleitungen nutzen.



Der Verlauf eines Letscall-Vishing-Angriffs.
(Bild: Threatfabric)

Mit den bei der Handy-Infektion erbeuteten sensiblen Informationen beantragen die Drahtzieher hinter der Betrugsmasche im Namen der Opfer einen Mikro-Kredit. Sofern Opfer ungewöhnliche Aktivitäten mitbekommen, rufen die Betrüger sie an und geben sich als Mitarbeiter des Bank-Sicherheits-Teams aus. Sie beschwichtigen die Opfer, dass sie sich keine Sorgen machen müssten.

Versucht ein Opfer, die Bank selbst anzurufen, um Fragen zu den verdächtigen Aktivitäten zu stellen, leiten die Betrüger den Anruf an von ihnen kontrollierte Callcenter um. Ein gut vorbereiteter Mitarbeiter beantwortet den Anruf und könne zudem weitere Informationen ausforschen, die den Drahtziehern bei ihren kriminellen Aktivitäten und dem Abschluss des betrügerischen Geldtransfers weiterhelfen.

Professionell aufgestellte Cyberkriminelle

Die Threatfabric-Forscher führen aus, dass die kriminelle Gruppe aus mehreren Spezialisten bestehen müsse. Sie benötigen Android-Entwickler mit Kenntnissen von VoIP-Routing, Webdesigner für Icons und Inhalte von Phishing-Seiten, Administrator-Panels und mobilen bösartigen Apps, Frontend-Entwickler mit Javascript-Kenntnissen einschließlich VoIP-Verkehr-Verarbeitung sowie Backend-Entwickler, die die Backend-APIs absichern. Außerdem gehören zur kriminellen Bande natürlich Call-Center-Mitarbeiter mit Social-Engineering-Skills, die zudem mehrere Sprachen fließend beherrschen.

(**dmk** [2])

URL dieses Artikels:

`https://www.heise.de/-9212374`

Links in diesem Artikel:

[1] https://www.threatfabric.com/blogs/letscall-new-sophisticated-vishing-toolset

[2] mailto:dmk@heise.de