Bild: KI Midjourney | Collage c't

Konten-Phishing 3.0

Wie organisierte Kriminalität Bankkunden ausplündert

Code-Frickeleien waren gestern, heute gibt es kommerzielle Phishing-Kits. Angreifer, die Onlinebanking-Kunden ins Visier nehmen, haben sich professionalisiert. Wir geben einen Überblick über deren Mittel, aber auch ihre Grenzen.

Von Markus Montz

Im Rückblick war es früher scheinbar so einfach: Phishing nach Onlinebanking- oder Kreditkartendaten wirkte durchweg dilettantisch, die Frage nach zehn TANs aus der gedruckten Liste war zu offensichtlich und die Hauptgefahr ging von Banking-Trojanern aus. Doch die Täter haben viel dazugelernt.

Heute findet Anti-Viren-Software zwar die meisten Banking-Trojaner. Die EU hat zudem Angriffe auf das Onlinebanking und bei Kartenzahlungen mit der obligatorischen Zwei-Faktor-Authentifizierung (2FA) deutlich erschwert. Als Reaktion operieren die Täter beim Phishing nun aber verstärkt arbeitsteilig und setzen mit immer mehr psychologischem Know-how auf das schwächste Glied in der Kette: arglose Nutzer. Dabei haben sie auch technisch aufgerüstet. Benötigten Verbrecher vor 15 Jahren noch gute IT-Security-Kenntnisse, helfen ihnen heute professionelle Tools. Damit sind Angriffe sowohl für Opfer als auch für Banken viel schwerer zu entdecken.

Phishing-Kit „V3B“

Zu den neueren Tools dieser Art gehört das Phishing-Kit „V3B“, das die kalifornische Sicherheitsfirma Resecurity analysierte und im Juni 2024 in ihrem Blog beschrieb (siehe ct.de/yqh3). Die Erstel-

ler sind demnach seit März 2023 unter dem Pseudonym „Vssrtje“ auf Telegram und in einschlägigen Darknet-Communities aktiv. Dort bewerben sie V3B und vertreiben es an andere Kriminelle. Allein der Telegram-Kanal hatte zuletzt über 1300 Abonnenten. Zu den Abnehmern zählen laut Resecurity vor allem eher erfahrene Cyberkriminelle.

V3B zielt auf Nutzer von Onlinebanking und Kreditkarten im Internet. Die Ersteller haben es auf europäische Bankkunden zugeschnitten (siehe Kasten „Angriffsziele“ auf S. 118). Das Phishing-Kit kann auf Fake-URLs täuschend echt wirkende Webseiten von Banken und Sparkassen bereitstellen. Über verschiedene Social-Engineering-Verfahren bringen die Betrüger ihre Opfer dazu, dort Informationen einzugeben. Dazu zählen Logindaten und Passwörter, bei Bedarf aber auch persönliche Daten wie Geburtsdaten, Telefonnummern oder Mailadressen. Ebenso können die Täter eingegebene TANs in Echtzeit abgreifen oder ihre Opfer dazu verleiten, 2FA-pflichtige Aktionen per Push-Bestätigung freizugeben.

Die kriminellen Kunden haben die Wahl zwischen zwei Abo-Modellen. Beim „Phishing as a Service“ (PhaaS) hostet Vssrtje die Software. Die Täter können V3B aber auch auf ihren eigenen Servern installieren. Updates und Kundensupport sind in beiden Modellen inbegriffen. Optional buchen die Täter Einzel- oder Paketmodule für Kreditinstitute hinzu. Pro Modul bezahlen die Abnehmer eine monatliche Abo-Gebühr zwischen derzeit 130 und 550 US-Dollar (letzteres für das komplette Deutschland-Paket) in Kryptowährungen.

Das Phishing-Kit besteht aus mehreren Komponenten. Die erste ist ein Backend, das szenariobasiert arbeitet und von Opfern eingegebene Zugangsdaten abfängt. Dazu kommt eine Komponente, die Webseiten und Pop-ups von Banken nachahmt und dem Opfer echt aussehende Login- beziehungsweise Anmeldeformulare präsentiert. Managen können die kriminellen Kunden von Vssrtje all das über ein benutzerfreundliches Admin-Dashboard namens „uPanel“ samt grafischer Benutzeroberfläche für Mobil- und Desktopgeräte. So brauchen sie kaum technische Vorkenntnisse, um die Echtzeitkommunikation mit ihren potenziellen Opfern durchzuführen.

Unter der Haube des Kits arbeitet ein angepasstes Content-Management-System (CMS). Der von ihm ausgelieferte Code ist laut Resecurity so gestaltet, dass gängige Anti-Malware-Programme sowie spezialisierte Suchbots und -maschinen nicht anschlagen und keine eindeutigen Erkennungsmerkmale finden können.

Angriff in Echtzeit

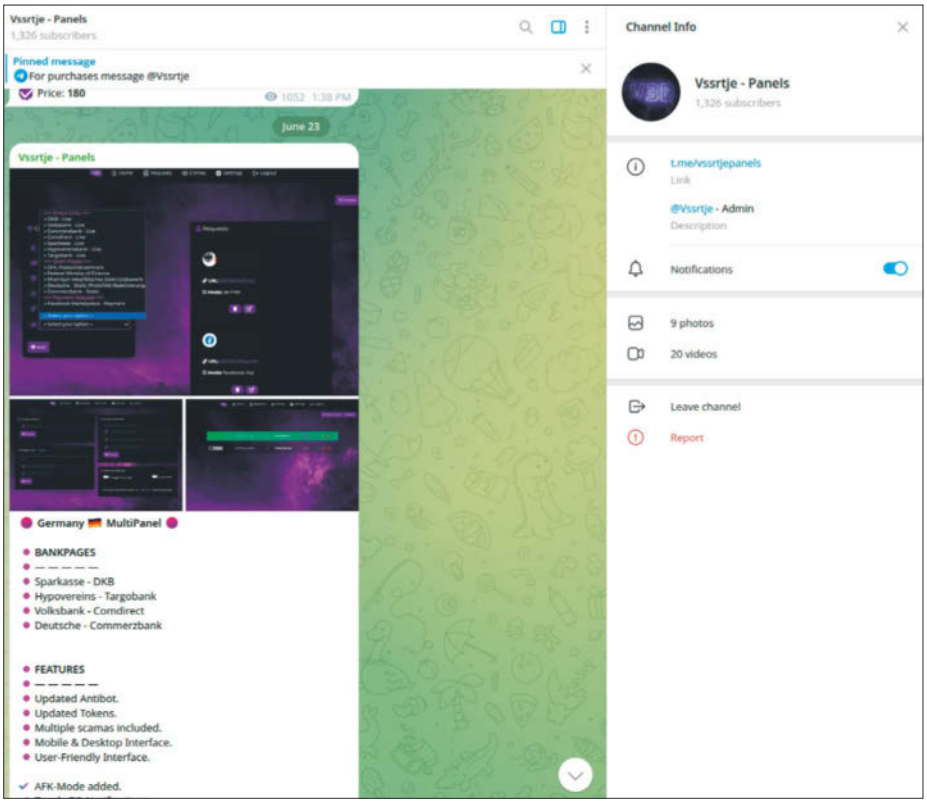
Ruft ein Opfer eine von V3B erzeugte Phishing-Seite auf, benachrichtigt das Kit die Betrüger in Echtzeit. Das Opfer bekommt zeitgleich eine Eingabemaske eingespielt. Zögert das Opfer, wenn es zum Beispiel Nutzernamen und Passwort für das Onlinebanking eintippen soll, können die Täter es über die integrierte Livechat-Funktion beeinflussen. Sobald das Opfer die Daten abgeschickt hat, bekommen die Täter sie im Klartext in uPanel angezeigt und über ein API in einen Telegram-Account gespielt.

Wenn die Täter sich damit bei der richtigen Onlinebanking-Website anmelden wollen, müssen sie aber die nun folgende 2FA überwinden. Dazu gaukelt V3B dem Opfer auf der Fakeseite das 2FA-Element vor und präsentiert dem Opfer irgendeine Ausrede, dass ein von ihm ausgelöster Vorgang die TAN-Eingabe oder Push-Freigabe erforderlich mache. In Wahrheit nutzen die Täter die Freigabe für ihre Zwecke. Wird das Opfer misstrauisch, weil es sorgfältig auf den auf seinem 2FA-Gerät angezeigten Empfänger oder Verwendungszweck achtet, können die Täter wieder über den Livechat Einfluss nehmen.

V3B „unterstützt“ SMS-TAN ebenso wie Push-Bestätigungen in einer Smartphone-Sicherheitsapp als zweiten Faktor. Das Phishing-Kit kann außerdem mit QR- oder Farbmatrix-Code umgehen. Die

c't kompakt

- Angriffe auf Onlinebanking-Kunden sind ausgeklügelter denn je, wie neu entdeckte Phishing-Kits zeigen.
- Einmal begonnene Angriffe mit solchen Kits verlaufen gut getarnt und sind schwer zu entdecken.
- Dennoch bleiben Lücken, die man mit genügend Vorwissen erkennen kann, sodass die Täter abtropfen.



Screenshot: Resecurity

Auf Telegram vertreibt „Vssrtje“ das Phishing-Kit V3B. Die Werbung für Deutschland zeigt auch die (mindestens) betroffenen Banken.

kopiert es mithilfe einer Browsererweiterung für die Täter von der Originalwebsite und spielt sie dem Opfer auf der Fakeseite ein. Dabei ist es egal, ob das Opfer ein Smartphone oder einen TAN-Generator zum Auslesen verwendet, weil der Zahlencode ja korrekt generiert und dann an die falsche Seite übertragen wird. Prinzipiell dürfte es auf diesem Weg auch möglich sein, andere Verfahren durchzuleiten, etwa die animierten Flickercodes des sogenannten chipTAN-Verfahrens, auch wenn Resecurity dies bisher nicht erwähnt. Einmal im Onlinebanking angemeldet, können die Täter dort weitere Aktionen wie eine Überweisung oder Limitänderung anstoßen. Im schlimmsten Fall schalten sie sich ein eigenes Gerät für die 2FA frei.

V3B lässt sich über uPanel mithilfe von Trigger-Funktionen und -Kombinationen in hohem Maße automatisieren, damit das Kit zahlreiche Aktionen koordiniert ausführt. Die Kriminellen müssen so nur noch punktuell selbst Hand anlegen, um beispielsweise Livechats mit ihren Opfern mit (vorgefertigten) Antworten zu befüllen. So können sie sogar mehrere Opfer parallel betrügen.

Über regelmäßige Updates hält Vssrtje die Tarnung von V3B und die generierten Fakeseiten aktuell. Das garantiert den kriminellen Kunden jederzeit eine passgenaue Unterstützung für die verschiedenen Geräte und Verfahren, die Banken ihren Kunden zur Zwei-Faktor-Authentifizierung anbieten.

Die Phishing-Branche

V3B ist nur ein Beispiel für derartige Phishing-Kits, von denen es zahlreiche weitere mit unterschiedlicher Technik gibt. Mit dem zum Pentesting beworbenen Tool „Evilginx“ kann man sich nach einer erfolgreichen Phishing-Attacke als Man-in-the-Middle zwischen das Opfer und den Bankserver schieben und neben anderen Eingaben auch schlecht geschützte Session Cookies abfangen. Die nutzen Banken vor allem, damit ihre Kunden beim Onlinebanking-Login nur alle paar Monate den 2FA-Prozess durchlaufen müssen.

Andere Tools wie „EvilProxy“ duplizieren gleich die komplette Banking-Website, wobei die Täter Kontostände oder Umsatzdaten mit erfundenen Werten austauschen, um Opfer in Sicherheit zu wiegen. Auch Banking-Trojaner sind trotz des vor allem in Windows verbesserten Malware-Schutzes nicht ganz ausgestorben. Sie manipulieren beispielsweise die Anzeige direkt auf dem PC oder Smartphone.

Gerne arbeiten Täter auch mit QR-Codes in Mails oder auf präparierten Websites, die dann auf die Phishing-Seiten führen. Anders als Hyperlinks erkennt ein Anti-Phishing-Scanner solche manipulativen Grafikelemente meist nicht. Tools wie „EvilQR“ verschleiern ihr Werk dabei durch mehrfache Weiterleitung sowohl vor den Nutzern als auch vor misstrauischen Prüfroutinen.

Unter dem Begriff „Crime as a Service“ hat sich um solche Tools eine arbeitsteilige und hoch spezialisierte Branche gebildet. Ihre Mitarbeiter bekommen Gehälter, Schulungen, Sozialleistungen und Büros, denn bereits die Programmierung von Tools wie V3B kann überaus profitabel sein. Die eigentlichen Betrüger können niedrigschwellig von überall auf der Welt agieren. Dank der gut ausgebauten Infrastruktur und der professionellen Tools skalieren ihre Attacken leicht. Dadurch hat sich die Zahl der Angreifer und damit die der Angriffe drastisch erhöht.

Opfer werden mit Phishingmails, per SMS („Smishing“), über WhatsApp und andere Messenger, die besagten Webseiten oder andere Social-Engineering-Tricks geködert. Erst die darin enthaltenen Links führen die Opfer auf die von V3B & Co. erzeugten Phishing-Seiten. Eine weitere Variante sind authentisch wirkende Anrufe mit gefälschter Telefonnummer („Call ID Spoofing“), in deren Verlauf die Betrüger ihre Opfer über parallel verschickte Mails, Textnachrichten oder Kurzlinks in die Falle locken.

Sprachbarrieren gibt es kaum noch, KI-gestützte Übersetzungen erzeugen geschliffene Formulierungen. Mit Sprach-KIs können Betrüger sogar die Stimmen von Bankberatern imitieren. Die Betrüger verdienen dabei gut und können es sich daher leisten, die Technik und Ressourcen für das professionelle Phishing einzukaufen. Neben den Phishing-Kits erwerben sie beispielsweise Datenbanken mit hunderttausenden gestohlenen Mailadressen, Telefonnummern und Namen, aber auch Listen mit Passwörtern, IBAN, Kreditkarten- und anderen sensiblen Daten. Mithilfe weiterer Software fließen diese Informationen in massenhaft versandte Phishing-Mails, Textnachrichten oder Anrufe aus speziellen Callcentern. Wenn sie an passende Daten kommen, können Kriminelle außerdem Zweit-SIM-Karten bestellen und damit SMS-TANs der Opfer abfangen („SIM Swapping“).

Auch für die Geldwäsche greifen die Täter auf externe Spezialisten zurück. Diese besorgen die erforderlichen Bankkonten, indem sie beispielsweise sogenannte Finanzagenten („Money Mules“) anheuern. Die stellen gegen Provision ihr Konto wissend oder unwissend zur Verfügung. Geht Geld ein, kaufen die Täter oder Finanzagenten davon Kryptowährungen, digitale Gutscheine oder sie überweisen die Beute auf Konten im Ausland.

Angriffe abwehren

Trotz ihrer fortschrittlichen Werkzeuge sind die Täter für ihren Betrug auf Lücken und Unachtsamkeit in den Sicherheitsmaßnahmen angewiesen. Wenn ein Opfer der Phishing-Mail, der Textnachricht auf dem Handy oder dem einen Fake-Anruf keinen Glauben schenkt, nützt das schönste Phishing-Dashboard nichts. Zudem ist immer ein Link zur Phishing-Seite im Spiel, der einer genauen Prüfung seines

Angriffsziele

Die Kriminellen können in V3B Module für mindestens 54 europäische Banken und Bankengruppen hinzubuchen. Gefährdet sind sowohl das Onlinebanking als auch die Online-Verwendung von Visa- oder Mastercard-Karten, die diese Banken herausgeben.

Für Deutschland nennt V3B-Entwickler Vssrtje aktuell Comdirect, Commerzbank, Deutsche Bank, DKB, HypoVereinsbank, Sparkassen, Targobank und Volksbanken. Indirekt könnten damit auch die Norisbank, die Postbank sowie die Raiffeisen- und weitere Genossenschaftsbanken betroffen sein. Aus dem europäischen Kontext ergeben sich außerdem die Digitalbank Bunq, die ING, die Santander und ICS Cards („Visa World Card“).

Unter den Instituten aus Österreich befinden sich Bank99, BAWAG, DADAT, Dolomitenbank, EasyBank, Erste Sparkasse (George), Santander, Spardabank sowie die Volksbanken und Raiffeisenbanken. Die Schweiz erwähnt Vssrtje nicht.

Ziels nicht standhält. Zwar investieren die Täter viel in Glaubwürdigkeit, damit ihre Opfer die Phishing-Seiten trotzdem aufrufen, aber da die Kontaktaufnahme meist nach dem Gießkannenprinzip erfolgt, halten sie die Texte oft allgemein und unpersönlich. Das tun seriöse Absender wie Banken und Behörden so nicht.

Doch Obacht: Selbst eine persönliche Anrede oder gar die mitgeschickte IBAN können Teil einer Falle sein. Solche Angaben finden nach Datendiebstählen ihren Weg auf Darknet-Marktplätze. Gehen die Täter davon aus, dass sich der Aufwand lohnt, weil bei einem Opfer viel zu holen ist, recherchieren sie zudem auf sozialen Medien oder im Netz oder rufen an und erschleichen sich durch geschickte Gesprächsführung Details. Das gilt besonders auch für Unternehmen. Mit diesem Wissen können die Täter ihr Phishing individuell zuschneiden („Spearphishing“).

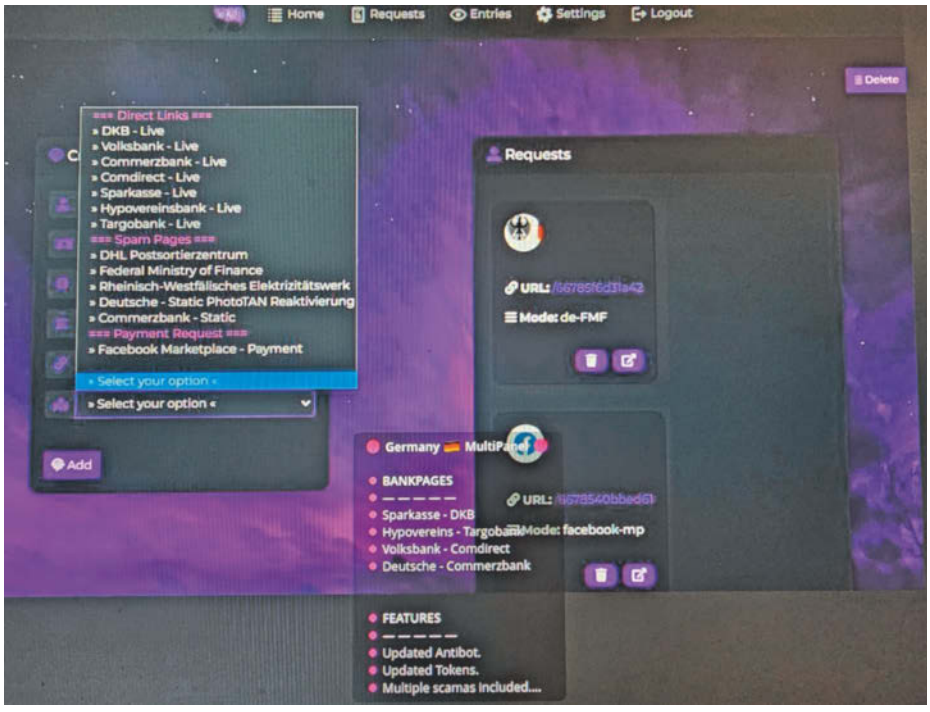
In den Texten oder Anrufen geben die Täter vor, eine offizielle Stelle oder ein Unternehmen zu sein. Neben dem Kreditinstitut selbst kommen Polizei-, Zoll- und andere Behörden infrage, auch Paketdienste oder ein „Kundensupport“ sind beliebt. In ihrer Kommunikation erzeugen sie immer Handlungsdruck und drohen mit finanziellen Verlusten, Kontosperrungen oder gar strafrechtlichen Folgen, wenn das Opfer nicht schnell aktiv wird. Es soll keine Zeit zum Denken bleiben. So arbeiten seriöse Absender oder Anrufer jedoch nicht.

Beispielsweise behaupten die Täter, das Onlinebanking sei kompromittiert worden oder die Bank oder die Polizei habe eine verdächtige Überweisung blockiert. Oder sie fabulieren, eine dritte Person habe versehentlich Geld auf das Konto überwiesen und müsse es zurückerhalten. Alle drei Fälle können tatsächlich eintreten, aber man bekäme immer genug Zeit, um die Angaben in Ruhe zu prüfen.

Weitere Szenarien sind frei erfundene Updates von Banking-Software oder -Apps oder eine angeblich erforderliche Reaktivierung der Sicherheitsapp oder des Onlinebankings. Auch neue AGB, Nutzungsbedingungen oder Datenschutzerklärungen sind als Geschichten beliebt, ebenso Sparzins- oder Anlageangebote, angebliche Nachrichten von DHL & Co. über Pakete mit Adress- oder Zollproblemen. Allen ist gemein, dass echte Absender nie Links zu Dateneingabemasken schicken würden.

Ein letzter Schutzwall bleibt die Zwei-Faktor-Authentifizierung. Das genutzte Gerät, ob Smartphone oder TAN-Generator, zeigt den Zweck der Freigabe an. Das gilt für das Login ins Onlinebanking oder die Aktivierung einer digitalen Karte ebenso wie für die Ziel-IBAN und den Betrag bei einer Überweisung. Diese Anzeige können die Täter nicht manipulieren. Bei Abweichungen oder auch nur Unklarheiten sollte man abbrechen und das Onlinebanking oder die Karte vorsorglich sperren lassen. Das gilt ganz besonders dann, wenn jemand am Telefon oder im Livechat etwas anderes sagt: Kein echter Bankmitarbeiter, geschweige denn Polizist würde zu einer 2FA auffordern und erst recht keine Diskrepanzen begründen.

Solche Phishing-Nachrichten sind typische Aufhänger, mit denen die Täter ihre Opfer auf die Fake-Seiten ziehen.



Screenshot: Resecurity

Mithilfe eines grafischen Dashboards können die Täter den kompletten Phishing-Prozess in Echtzeit steuern.

Fazit

Onlinebanking-Kunden sehen sich heute einer professionellen, hochgradig professionalisierten kriminellen Industrie gegenüber, die an ihr Geld will. Doch die Täter sind schlagbar, wenn alle ihren Teil beitragen. Die Nutzer und ihre Sorgfalt haben wir angesprochen. Sie sind aber nur ein Glied in der Kette.

Gefordert sind auch Banken, die ihre Mitarbeiter (und übrigens auch Kunden) noch gezielter schulen sollten und auch mehr in Authentifizierungs- und Prüfungssysteme investieren könnten. Plattformen und Telekommunikationsanbieter müssen verhindern, dass Betrüger mit gefälschten Nummern anrufen können und URL-Namen wie „ssparkasse.de“ überhaupt online gehen. Auch die Politik ist mit guten Ideen gefragt, nicht zuletzt bei der Ausstattung ihrer Strafverfolgungsbehörden. *(mon@ct.de)* c't

Resecurity-Blogeintrag: ***ct.de/yqh3***