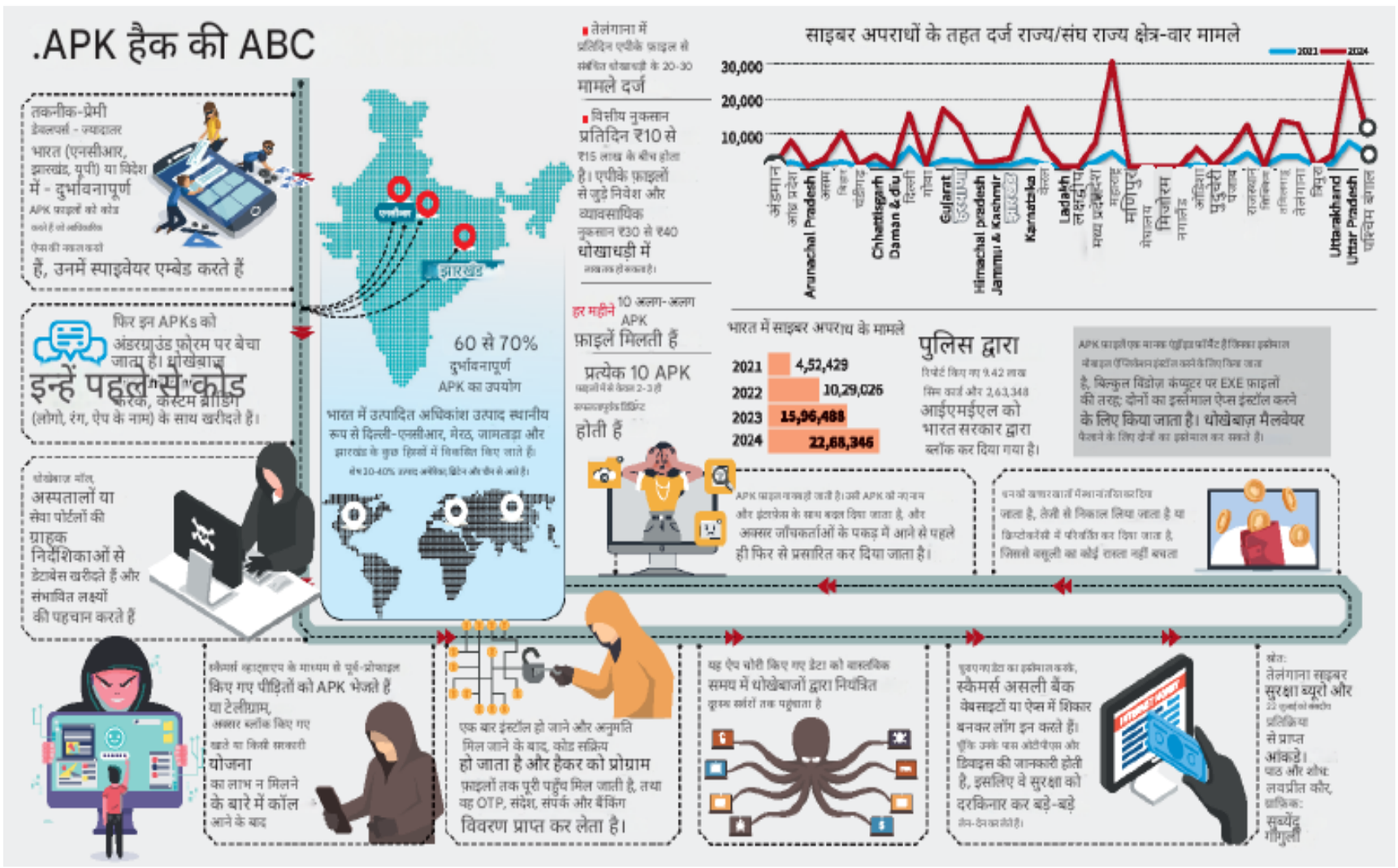
CACHE



एपीके घोटाले के अंदर: वित्तीय धोखाधड़ी के लिए नकली ऐप्स का उपयोग कैसे किया जाता है

एपीके धोखाधड़ी आज देश में सबसे तेज़ी से बढ़ते साइबर अपराध खतरों में से एक है। दुर्भावनापूर्ण एंड्रॉइड पैकेज किट (एपीके) फ़ाइलों द्वारा संचालित ये घोटाले, डिजिटल सिस्टम में जनता के विश्वास का फायदा उठाते हैं और राज्य की सीमाओं के पार छिपे रहने और सक्रिय रहने के लिए अत्याधुनिक तकनीकी उपकरणों का इस्तेमाल करते हैं।

अब तक की कहानी:
हज़ारों मोबाइल फ़ोन वाले भारतीय किसी कॉल का जवाब देने या किसी मैसेज पर क्लिक करने के बाद पैसे गँवा रहे हैं। कभी-कभी इसकी शुरुआत एक शांत, विनम्र और ज़रूरी फ़ोन कॉल से होती है। दूसरी तरफ़ से आवाज़ किसी बैंक खाते के ब्लॉक होने, सरकारी सब्सिडी छूट जाने या बिजली के बिल के बारे में चेतावनी देती है। कुछ ही देर बाद, एक मैसेज आता है जिसमें एक ऐप का लिंक होता है जो तुरंत समाधान का वादा करता है। ऐप आधिकारिक लगता है, एक विश्वसनीय संस्थान का लोगो लगा होता है, और बिना किसी समस्या के इंस्टॉल हो जाता है। उपयोगकर्ता कुछ सामान्य अनुमतियाँ देता है - संपर्क, एसएमएस, सूचनाएँ - बिना यह जाने कि उसी पल उनका फ़ोन एक खुली तिजोरी बन गया था।

ऐप इंस्टॉल करने के बाद क्या होता है?
10 मिनट से भी कम समय में, बैंक खातों से पैसे गायब होने लगते हैं। फिक्स्ड डिपॉज़िट समय से पहले बंद हो जाते हैं, और ओटीपी इंटरसेप्ट हो जाते हैं। ऐप, जो अब बैकग्राउंड में चलता है, लोकेशन से लेकर निजी संदेशों तक, सब कुछ मॉनिटर, मिरर और माइन करता है। उपयोगकर्ता को तब तक पता नहीं चलता जब तक बहुत देर हो चुकी होती है। और जब तक मदद मांगी जाती है, तब तक धनराशि डिजिटल लॉन्ड्रिंग की परतों से गुज़र चुकी होती है, जिसे वापस पाना असंभव होता है।

एपीके धोखाधड़ी आज देश में सबसे तेज़ी से बढ़ते साइबर अपराध के खतरों में से एक है। राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल ने पिछले छह महीनों में 12,47,393 विभिन्न प्रकार के मामले दर्ज किए हैं। संसद को सूचित किया गया है कि 2021 और 2025 के बीच साइबर अपराधों में 900% की वृद्धि हुई है। तेलंगाना साइबर सुरक्षा ब्यूरो (TGCSB) के आंकड़ों से पता चला है कि जनवरी से जुलाई 2025 के बीच कुल 2,188 ऐसे मामले सामने आए, जिससे ₹779.06 करोड़ का नुकसान हुआ। अधिकारियों ने बताया कि हर दिन ऐसे 20 से 30 मामले सामने आते हैं, जिनमें दैनिक वित्तीय नुकसान ₹10 से ₹15 लाख के बीच होता है। निवेश और व्यवसाय जैसे उच्च-दांव वाले घोटालों में, नुकसान ₹30 से ₹40 लाख तक जा सकता है। दुर्भावनापूर्ण एंड्रॉइड पैकेज किट (APK) फ़ाइलों द्वारा संचालित ये घोटाले, डिजिटल प्रणालियों में जनता के विश्वास का दुरुपयोग करते हैं और राज्यों की सीमाओं के पार छिपे रहने और सक्रिय रहने के लिए परिष्कृत तकनीकी उपकरणों का उपयोग करते हैं।

यह धोखाधड़ी कैसे काम करती है?
एंड्रॉइड उपकरणों पर APK फ़ाइलें, विंडोज़ कंप्यूटरों पर .exe फ़ाइलों की तरह ही होती हैं; दोनों का उपयोग ऐप्स इंस्टॉल करने के लिए किया जाता है, और धोखेबाज़ दोनों का उपयोग मैलवेयर फैलाने के लिए कर सकते हैं।

धोखेबाज़ इन ऐप्स को आधिकारिक पोर्टलों, जैसे पीएम-किसान जैसी सरकारी सब्सिडी योजनाओं, टैक्स रिफंड प्लेटफ़ॉर्म, बिजली बोर्ड, या केवाईसी अपडेट मांगने वाले बैंकों, के रूप और भाषा की नकल करने के लिए बनाते या स्रोत करते हैं। ये नकली ऐप्स अक्सर व्हाट्सएप जैसे सोशल मीडिया प्लेटफ़ॉर्म के माध्यम से प्रसारित होते हैं, और साथ में ऐसे संदेश भी होते हैं जो उपयोगकर्ताओं से तुरंत कार्रवाई करने का आग्रह करते हैं।

डेवलपर्स एन्क्रिप्शन तकनीकों का उपयोग करते हैं जो दुर्भावनापूर्ण कोड को पहचान उपकरणों से छिपाते हैं। इंस्टॉलेशन के दौरान निष्क्रिय रहने से, ये APK एंटीवायरस सॉफ़्टवेयर के स्कैन को दरकिनार कर देते हैं। डाउनलोड होने के बाद, ऐप कई अनुमतियाँ मांगता है, जिसमें संपर्कों, संदेशों, कॉल लॉग, स्थान, माइक्रोफ़ोन और सूचनाओं तक पहुँच शामिल है।

यह ऐप फ़ोन की प्रोग्राम फ़ाइलों तक पहुँच प्राप्त कर लेता है, रीयल-टाइम में डेटा एकत्र करता है और उसे एन्क्रिप्टेड बिट्स में धोखेबाज़ों द्वारा संचालित बाहरी सर्वरों तक पहुँचा देता है। ये बिट्स, हालाँकि आम उपयोगकर्ताओं के लिए पढ़ने योग्य नहीं होते, लेकिन बैंकिंग क्रेडेंशियल, ओटीपी, संपर्क और स्थान निर्देशांक जैसी बहुमूल्य जानकारी निकालने के लिए डिकोड किए जाते हैं।

इन ऐप्स का संचालन कौन करता है?
इन APKs को प्रसारित करने वाले धोखेबाज़ शायद ही इन्हें बनाने वाले होते हैं। बल्कि, ये ऐप्स एक सुव्यवस्थित भूमिगत अर्थव्यवस्था का हिस्सा हैं। साइबर अपराध अधिकारियों का अनुमान है कि भारत में इस्तेमाल होने वाले 60 से 70% दुर्भावनापूर्ण APK दिल्ली-एनसीआर, मेरठ, उत्तर प्रदेश, जामताड़ा और झारखंड के कुछ हिस्सों में तकनीकी रूप से दक्ष लोगों द्वारा स्थानीय स्तर पर विकसित किए जाते हैं। शेष 30-40% अंतरराष्ट्रीय स्तर पर उत्पन्न होते हैं, जिनके निशान अमेरिका, ब्रिटेन और चीन तक जाते हैं। टेलीग्राम चैनल और डार्क वेब मार्केटप्लेस प्रमुख वितरण चैनल के रूप में काम करते हैं, जो शुल्क के लिए पहले से निर्मित APK किट और मॉड्यूल प्रदान करते हैं।

एक बार प्रचलन में आने के बाद, उसी APK फ़ाइल को इंटरफ़ेस (फ़ाइल का नाम, लोगो और URL या वेब पता) में मामूली बदलावों के साथ दोबारा इस्तेमाल किया जाता है, जिससे पुराने संस्करणों को ब्लैकलिस्ट किए जाने के बाद भी इसे पहचाना नहीं जा सकता।

साइबर अपराध अधिकारियों का कहना है कि हर महीने सैकड़ों घोटाले के मामलों में, केवल लगभग 10 अलग-अलग APK फ़ाइलें ही मिलती हैं, जो कुछ दुर्भावनापूर्ण ऐप्स के व्यापक पुन: उपयोग की ओर इशारा करती हैं।

उपयोगकर्ताओं को कैसे निशाना बनाया जाता है?
शिकार का चुनाव बिल्कुल भी यादृच्छिक नहीं होता। किसी शारीरिक अपराध से पहले की जाने वाली रेकी की तरह, साइबर धोखेबाज़ हमला करने से पहले व्यापक डिजिटल निगरानी करते हैं।

टीजीसीएसबी के एक अधिकारी ने कहा, "धोखेबाज़ मॉल, अस्पतालों या सेवा पोर्टलों की ग्राहक निर्देशिकाओं से प्राप्त लीक हुए डेटाबेस खरीदते हैं, जो डार्क वेब, टेलीग्राम या यहाँ तक कि जस्ट डायल जैसे स्थानीय सर्च इंजनों पर आसानी से उपलब्ध होते हैं।" अधिकारी ने बताया, "इन डेटासेट में नाम, फ़ोन नंबर, ईमेल आईडी, पते और कभी-कभी आय या पेशेवर विवरण भी शामिल होते हैं, जो अपराधियों को अपना तरीका अनुकूलित करने में मदद करते हैं।"

डॉक्टर, बैंक कर्मचारी, शिक्षक और रियल एस्टेट एजेंट जैसे उच्च आय वाले पेशेवर अक्सर निशाने पर होते हैं। लक्ष्य के बारे में पहले से ज्ञात आंशिक जानकारी का उपयोग करके, धोखेबाज़ विश्वास को प्रभावित करने और त्वरित कार्रवाई करने के लिए विश्वसनीय, तत्काल संदेश तैयार करते हैं।

जांचकर्ता इस समस्या से कैसे निपट रहे हैं?
जब कोई धोखाधड़ी वाला ऐप ज़ब्त किया जाता है, तो साइबर फोरेंसिक टीमें सर्वर की उत्पत्ति का पता लगाने या डेवलपर के हस्ताक्षरों की पहचान करने के लिए उसे डिक्रिप्ट करती हैं। लेकिन परिणाम मिश्रित हैं। हर 10 APK में से केवल 2-3 ही सफलतापूर्वक डिक्रिप्ट हो पाते हैं। ज़्यादातर में केवल सर्वर एड्रेस या सामान्य कोड संरचनाएँ ही दिखाई देती हैं। फ़ाइलों में पहचान योग्य डेवलपर हस्ताक्षर बहुत कम होते हैं।

जब वित्तीय लेन-देन का पता लगाया भी जाता है, तो वे आमतौर पर खच्चर खातों, अस्थायी बैंक या वॉलेट खातों में पहुँच जाते हैं जिनका इस्तेमाल चोरी की गई धनराशि प्राप्त करने के लिए किया जाता है, जिसे जल्दी से क्रिप्टोकरेंसी में बदल दिया जाता है। गिरफ़्तारियाँ होती हैं, खासकर उन स्थानीय सहयोगियों की जो इन खच्चर खातों का प्रबंधन करते हैं या APK वितरित करते हैं। लेकिन मास्टरमाइंड और कोडर्स, खासकर जो विदेशी हैं, पकड़ से बाहर हैं।

जांचकर्ताओं की रिपोर्ट के आधार पर Google ने हाल के महीनों में लगभग 50 दुर्भावनापूर्ण ऐप्स हटाए हैं। अधिकारी ने बताया, "Google या कोई अन्य मध्यस्थ अपने सर्वर पर होस्ट किए जा रहे हर एप्लिकेशन की जाँच नहीं करता है। धोखेबाज सर्च इंजन पर होस्टिंग और प्रकाशन के लिए भुगतान करने हेतु खच्चर खातों और शेल पहचान का भी उपयोग करते हैं।"