ब्लैकरॉक एंड्रॉइड मैलवेयर

प्रीलिम्स के लिये

ब्लैकरॉक तथा इससे संबंधित अन्य सभी मैलवेयर

मेन्स के लिये

भारत की आंतरिक सुरक्षा में साइबर हमलों की चुनौती

चर्चा में क्यों?

हाल ही में थ्रेटफैब्रिक (ThreatFabric) नामक एक निजी कंपनी ने एंड्रॉइड फोन उपयोगकर्त्ताओं के लिये ब्लैकरॉक (BlackRock) नाम के एक नए एंड्रॉइड मैलवेयर से संबंधित चेतावनी जारी की है, जो कि मोबाइल फोन उपयोगकर्त्ताओं की संवेदनशील जानकारी चुराने में सक्षम है।

प्रमुख बिंदु

- इस मैलवेयर को लेकर जारी सूचना के अनुसार, यह अमेज़न, फेसबुक, जी-मेल (Gmail) और टिंडर (Tinder) समेत लगभग 377 स्मार्टफोन एप्लिकेशन से पासवर्ड और क्रेडिट कार्ड संबंधी संवेदनशील जानकारी प्राप्त करने में सक्षम है।
- चूँकि उपरोक्त सभी स्मार्टफोन एप्लिकेशन आम उपयोगकर्त्ताओं के बीच काफी लोकप्रिय हैं, इसलिये साइबर सुरक्षा विशेषज्ञ इस मैलवेयर से उत्पन्न खतरे को काफी गंभीर मान रहे हैं।

ब्लैकरॉक एंड्रॉइड मैलवेयर

- साइबर विशेषज्ञों के अनुसार, ब्लैकरॉक एंड्रॉइड मैलवेयर कोई नया मैलवेयर नहीं है, बल्कि यह 'ज़ेरेस मैलवेयर (Xeres Malware) के लीक हुए सोर्स कोड (Source Code) पर आधारित है।
- ब्लैकरॉक और अन्य एंड्रॉइड बैंकिंग मैलवेयर के बीच सबसे बड़ा अंतर यह है कि ये पहले से मौजूद सभी मैलवेयरों की तुलना में अधिक एप्स को लक्षित कर सकता है।
- ध्यातव्य है कि यह मैलवेयर किसी नए एप्लीकेशन को डाउनलोड करते समय ही उसी के साथ हमारे फोन में प्रवेश करता हैं।

ब्लैकरॉक एंड्रॉइड मैलवेयर का इतिहास

- दरअसल सबसे पहले वर्ष 2016 के अंत में लोकीबॉट (LokiBot) नाम से एक मैलवेयर सामने आया था, कुछ समय पश्चात् जब मैलवेयर के निर्माता को विभिन्न मंचों पर प्रतिबंधित कर दिया गया तो उसने इस मैलवेयर के सोर्स कोड (Source Code) को लीक कर दिया।
- वर्ष 2018 के शुरुआती माह में मिस्ट्रीबॉट (MysteryBot) मैलवेयर को सक्रिय होते हुए देखा गया, यद्यपि यह लोकीबॉट मैलवेयर पर ही आधारित था, किंतु इसे नए एंड्रॉइड संस्करणों (Android Versions) पर कार्य करने के लिये अपग्रेड किया गया था, साथ ही इसमें व्यक्तिगत जानकारी चोरी करने के लिये नई तकनीकों का भी इस्तेमाल किया गया था।
- वर्ष 2018 की दूसरी तिमाही में मिस्ट्रीबॉट मैलवेयर के उत्तराधिकारी के रूप में पैरासाइट (Parasite) नाम से एक नया मैलवेयर सामने आया, जिसमें कुछ नए फीचर शामिल थे।
- मई 2019 में एक्सरेस (Xeres) नाम से एक नया मैलवेयर आया, जो कि प्रत्यक्ष रूप से पैरासाइट मैलवेयर पर और अप्रत्यक्ष रूप से लोकीबॉट मैलवेयर पर आधारित थे, जब साइबर सुरक्षा से संबंधी विभिन्न मंचों पर यह मैलवेयर असफल रहा तो इसके निर्माता ने भी इसके सोर्स कोड (Source Code) को सार्वजनिक कर दिया।
- अंततः एक्सरेस मैलवेयर के सोर्स कोड का प्रयोग करते हुए ब्लैकरॉक नाम का मैलवेयर बनाया गया, इस मैलवेयर की सबसे बड़ी विशेषता यह है कि यह सोशल मीडिया एप्स जैसे- फेसबुक तथा जी-मेल और नेटवर्किंग एप्स जैसे- टिंडर आदि को लक्षित करता है।

कैसे कार्य करता है यह मैलवेयर?

- ब्लैकरॉक मैलवेयर भी अधिकांश एंड्रॉइड मैलवेयर की तरह ही कार्य करता है, एक बार फोन में इनस्टॉल (Install) होने के पश्चात् यह लक्षित एप की निगरानी करता है और जब उपयोगकर्त्ता लॉगिन अथवा क्रेडिट कार्ड संबंधी संवेदनशील जानकारी का प्रयोग करता है, तो यह मैलवेयर इस संवेदनशील जानकारी को अपने सर्वर के पास भेज देता है।
- यह मैलवेयर किसी भी एंड्रॉइड फोन के 'एक्सेसबिलिटी फीचर' (Accessibility Feature) का उपयोग करता है।
- जब मैलवेयर पहली बार एंड्राइड फोन पर लॉन्च किया जाता है, तो यह स्वयं ही एप्स की सूची से अपने आइकन (Icon) छिपा लेता है, जिसके कारण फोन उपयोगकर्त्ता के लिये यह अदृश्य हो जाता है और एक आम उपयोगकर्त्ता के लिये इसे पहचानना लगभग असंभव हो जाता है।
- साइबर विशेषज्ञों के अनुसार, ब्लैकरॉक मैलवेयर केवल ऑनलाइन बैंकिंग एप्स तक सीमित नहीं है, बल्कि यह अन्य श्रेणियों से संबंधित एप्स जैसे- व्यवसाय, कम्युनिकेशन, मनोरंजन, संगीत और समाचार एवं पत्रिका आदि को भी लक्षित कर सकता है।

क्या होता है मैलवेयर?

- मैलवेयर, किसी कंप्यूटर को नुकसान पहुँचाने के उद्देश्य से निर्मित किया जाने वाला एक प्रकार का सॉफ्टवेयर होता है, जो कंप्यूटर से संवेदनशील जानकारी चुरा सकता है और धीरे-धीरे कंप्यूटर को धीमा कर सकता है।
- इस प्रकार के कंप्यूटर सॉफ्टवेयर का निर्माण ही किसी कंप्यूटर उपकरणों को नुकसान पहुँचाने और संवेदनशील व्यक्तिगत जानकारी चुराने के उद्देश्य से किया जाता है।
- आमतौर पर मैलवेयर का निर्माण हैकर के समूहों द्वारा किया जाता है, जो कि अधिकांशतः इसका प्रयोग अधिक-से-अधिक पैसा कमाने के लिये करते हैं। इस कार्य के लिये वे या तो स्वयं मैलवेयर को अन्य कंप्यूटरों तक फैला सकते हैं अथवा वे इसे डार्क वेब (Dark Web) पर बेंच सकते हैं।
- हालाँकि यह ज़रूरी नहीं है कि मैलवेयर का निर्माण सदैव नुकसान पहुँचाने के उद्देश्य से ही किया जाए, कभी-अभी साइबर सुरक्षा विशेषज्ञ, सुरक्षा संबंधी परीक्षण करने के लिये भी मैलवेयर का निर्माण करते हैं, जिसे कार्य पूरा होने के पश्चात् नष्ट कर दिया जाता है।

बचाव संबंधी उपाय

- यह नया मैलवेयर इतना शक्तिशाली है कि यह एंटी-वायरस एप्लीकेशन को भी असफल कर सकता है। साइबर सुरक्षा विशेषज्ञों के अनुसार, मैलवेयर इनस्टॉल होने के पश्चात् यदि फोन उपयोगकर्त्ता किसी एंटी-वायरस सॉफ्टवेयर का प्रयोग करता है तो यह मैलवेयर उसे वापस होम स्क्रीन (Home Screen) पर रीडायरेक्ट कर देगा अर्थात उसे वापस होम स्क्रीन पर पहुँचा देगा।
- आवश्यक है कि किसी भी एप को विश्वसनीय स्रोतों जैसे गूगल प्ले स्टोर (Google Play Store) आदि से ही डाउनलोड किया जाए, अथवा इस कार्य के लिये कंपनी की आधिकारिक वेबसाइट का प्रयोग किया जाए।
- इसके अलावा एक मज़बूत पासवर्ड का प्रयोग किया जाए, स्पैम और फिशिंग आदि से सावधानी बरती जाए और किसी भी एप्लीकेशन को अनुमति देने से पूर्व उसके संबंध में जानकारी प्राप्त की जाए।

स्रोत: इंडियन एक्सप्रेस

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/what-is-blackrock-android-malware-and-are-you-vulnerable