शीर्षक:

नवीन सुरक्षा उपायों के साथ रैनसमवेयर के खतरों से निपटना

प्रिय बहुमूल्य ग्राहक,

रैनसमवेयर हमला एक साइबर हमला है जिसमें हैकर पीड़ित के डेटा को एन्क्रिप्ट करते हैं और इसे डिक्रिप्ट करने के लिए भुगतान की मांग करते हैं। यह संक्रमित लिंक या संलग्नक के माध्यम से फैलता है। यह उपयोगकर्ताओं को उनके सिस्टम से तब तक लॉक कर देता है जब तक वे फिरौती नहीं देते आमतौर पर फिरौती क्रिप्टोकरेंसी में ली जाती है।

इन हमलों से वित्तीय नुकसान होता है, परिचालन बाधित होता है, तथा संवेदनशील जानकारी से समझौता होता है, जिससे दुनिया भर में व्यवसायों, सरकारों और व्यक्तियों के लिए गंभीर खतरा पैदा होता है।

काम करने का ढंग:

- धमकी देने वाले लोग वैध फाइलों (जैसे, पीडीएफ, ऑफिस दस्तावेज) के रूप में दुर्भावनापूर्ण लिंक या संलग्नक के साथ ईमेल भेजते हैं। वे वैध वेबसाइटों पर दुर्भावनापूर्ण विज्ञापनों का भी उपयोग करते हैं जो पीड़ितों को रैनसमवेयर होस्ट करने वाली वेबसाइटों पर पुनर्निर्देशित करते हैं।

- सिस्टम पर एक बार निष्पादित होने के बाद, रैनसमवेयर मजबूत एन्क्रिप्शन एल्गोरिदम का उपयोग करके फ़ाइलों को एन्क्रिप्ट करना शुरू कर देता है। एन्क्रिप्ट की गई फ़ाइलें पीड़ित के लिए अप्राप्य हो जाती हैं, जिसे फ़ाइलों को डिक्रिप्ट करने के लिए क्रिप्टोकरेंसी (जैसे, बिटकॉइन) में भुगतान की मांग करते हुए फिरौती का नोट मिलता है।

- धोखेबाज फिरौती देने का निर्देश देते हैं और अक्सर फाइलों को डिलीट करने या डार्क-वेब पर बेचने की धमकी देते हैं।

- फिरौती देने से फ़ाइल पुनर्प्राप्ति या मैलवेयर हटाने की गारंटी नहीं मिलती है, और इससे आगे के हमलों को बढ़ावा मिलता है।

सावधानियां:

- महत्वपूर्ण फाइलों का नियमित रूप से बाहरी हार्ड ड्राइव या क्लाउड स्टोरेज सेवा पर बैकअप सुनिश्चित करें।

- कमजोरियों से बचाव के लिए ऑपरेटिंग सिस्टम, एंटीवायरस सॉफ्टवेयर और वैध वेबसाइटों के अनुप्रयोगों को नियमित रूप से अपडेट करें।

- अज्ञात या संदिग्ध प्रेषकों से प्राप्त ईमेल में संलग्नक खोलने या लिंक पर क्लिक करने से बचें।
- रैनसमवेयर और अन्य मैलवेयर खतरों का पता लगाने और उन्हें रोकने के लिए लाइसेंस प्राप्त और प्रभावी एंटीवायरस सॉफ़्टवेयर स्थापित करें और उसे अद्यतन रखें।

- फ़िशिंग प्रयासों को पहचानना सीखें, जहां हमलावर आपसे संवेदनशील जानकारी प्राप्त करने या मैलवेयर इंस्टॉल करने के लिए आपको धोखा देने का प्रयास करते हैं।

- केवल विश्वसनीय स्रोतों से ही सॉफ़्टवेयर और फ़ाइलें इंस्टॉल करें। कुछ भी डाउनलोड करने से पहले वेबसाइट की प्रामाणिकता की पुष्टि करें।

साइबर सुरक्षा जागरूकता पर अधिक जानकारी के लिए, बीओआई साइबर स्टार ई- मैन्युअल देखें या हमारी वेबसाइट के सुरक्षित बैंकिंग खंड पर जाएं।

हमारी वेबसाइट के शिकायत अनुभाग के अंतर्गत साइबर धोखाधड़ी की रिपोर्ट करें और साथ ही, भारत सरकार के पोर्टल: www.cybercrime.gov.in पर भी रिपोर्ट करें या 1930 पर कॉल करें।

बैंक ऑफ़ इंडिया BOI
Bank of India

सूचना सुरक्षा टीम