नेपाल सरकार

सञ्चार तथा सूचना प्रविधि मन्त्रालय

राष्ट्रिय साइबर सुरक्षा केन्द्र

सिंहदरबार, काठमाडौं

एडभाइजरी नं. NCSC-1146-112-03 मिति: २०८३/०१/०७

Ransomware आक्रमणबाट सुरक्षित रहनका लागि जारी गरिएको साइबर सुरक्षा एडभाइजरी

Ransomware त्यस्तो Software हो, जसको आक्रमणमा कम्प्युटर, मोबाइल वा अन्य Device वा यसमा रहेका फाइल/डाटालाई Lock/Encrypt गरी पहुँच अवरुद्ध गर्छ र सो फाइल/डाटालाई पुनः प्राप्त गर्नको लागि फिरौती (Ransom) माग गर्दछ। हालका दिनहरुमा सूचना प्रविधि प्रणालीहरुमा Ransomware आक्रमणका घटनाहरू उल्लेखनीय रुपमा वृद्धि भइरहेका छन्। सर्वसाधारण नागरिकलाई यस प्रकारका आक्रमणबाट हुन सक्ने क्षतिबाट बच्नको लागि सचेत गराउने उद्देश्यले यो एडभाइजरी जारी गरिएको छ।

१. Ransomware के हो?

१.१. यो एक प्रकारको हानिकारक सफ्टवेयर (Malware) हो, जसले तपाईंको फाइल वा सिस्टमलाई लक (Lock) वा इन्क्रिप्ट (Encrypt) गरी खोल्नै नदिने वा खुले पनि प्रयोग गर्न नसकिने बनाउँछ। फाइल वा सिस्टममा पुनः पहुँच प्राप्त गर्नको लागि फिरौती (Ransom) माग गर्दछ।

२. Ransomware ले तपाईंलाई के असर गर्न सक्छ?

२.१. तपाईंको महत्वपूर्ण डाटा, फाइल, कागजात वा पूरै उपकरणमा पहुँच रोक्न सक्छ।

२.२. तपाईंको संस्था/निकायले प्रदान गरेका सेवाहरु अवरुद्ध हुन सक्छ।

२.३. तपाईंको महत्वपूर्ण र संवेदनशील डाटा/सूचना चोरी वा लिक हुन सक्ने भएकोले गोपनीयता सम्बन्धी जोखिम हुन सक्छ।

२.४. तपाईंको डाटा/सूचना Unlock वा पूनर्प्राप्तिको लागि फिरौती माग्ने हुँदा आर्थिक नोक्सानी हुन सक्दछ।

३. के गर्दा Ransomware ले तपाईंको डाटामा आक्रमण गर्न सक्दछ?

३.१. इमेलहरुमा रहेका शंकास्पद Attachment हरु (PDF, Word, ZIP आदि) खोल्दा।

३.२. सामाजिक सञ्जाल, एस.एम.एस. (SMS) वा इमेल मार्फत आउने नक्कली वेबसाइट र शंकास्पद लिङ्कमा क्लिक गर्दा।

३.३. असुरक्षित स्रोतहरुबाट .exe/.apk फाइलहरु डाउनलोड गर्दा ।

३.४. Malware हरु लुकेर बसेको हुन सक्ने हुँदा Pirated/Cracked सफ्टवेयरहरु प्रयोग गर्दा।

३.५. Operating System लगायत प्रयोग गरिएका Software हरु नियमित Update नगर्दा।

३.६. Antivirus लगायत उपयुक्त सुरक्षा प्रणाली नहुँदा।

३.७. असुरक्षित नेटवर्क र USB/external device प्रयोग गर्दा।

४. Ransomware बाट जोगिन के गर्ने?

४.१. अपरिचित व्यक्ति वा स्रोतबाट प्राप्त ईमेलहरुमा रहेका शंकास्पद Link तथा Attachment खोल्दा ईमेल प्रेषक र Link तथा Attachment को आधिकारिकता सुनिश्चित भएपछि मात्र खोल्नुहोस्।

४.२. .exe/.apk जस्ता Executable File वा सफ्टवयरहरु Download गर्दा Google Play Store/Apple App Store/Microsoft Store वा सम्बन्धित सफ्टवेयरको आधिकारिक Website मात्र प्रयोग गर्नुहोस् ।

४.३. Cracked/Pirated लगायत अनधिकृत सफ्टवेयरहरु प्रयोग नगर्नुहोस्। सिस्टमलाई नियमित रुपमा अपडेट गर्नुहोस् र Antivirus लगायत उपयुक्त सुरक्षा प्रणालीको प्रबन्ध मिलाउनुहोस्।

४.४. डाटाको नियमित ब्याकअप गर्नुहोस्। ब्याकअपलाई क्लाउड र बाह्य स्टोरेज (Offline Storage) मा समेत सुरक्षित राख्नुहोस्।

४.५. नेटवर्कको सुरक्षा बलियो बनाउनुहोस्।

४.६. USB/External Device Malware नभएको सुनिश्चित गरी सावधानीपूर्वक प्रयोग गर्नुहोस्।

५. यदि Ransomware आक्रमण भई हालेमा के गर्ने?

५.१. Ransomware लागेको शंका लागेमा सो Malware अन्य उपकरणहरुमा फैलन नदिन तुरुन्तै उक्त उपकरणलाई इन्टरनेट/इन्ट्रानेटबाट अलग गर्नुहोस्।

५.२. इमेल, System Login आदिको पासवर्ड तुरुन्त परिवर्तन गर्नुहोस्।

५.३. आक्रमणकारीले माग गरेको रकम तुरुन्त नतिर्नुहोस्। रकम तिरेपछि पनि डाटा फिर्ता हुने सुनिश्चित हुँदैन। यसले आक्रमणकारीलाई झन् प्रोत्साहन दिनुका साथै भविष्यमा पुनः आक्रमण हुनसक्ने जोखिम बढाउँछ।

५.४. Backup बाट System Restore गर्नुहोस् । घटनाको विस्तृत विवरणसहित नेपाल प्रहरीको Cyber Bureau मा रिपोर्ट गर्नुहोस् र राष्ट्रिय साइबर सुरक्षा केन्द्रमा समेत जानकारी गराउनुहोस्।

५.५. Ransom Note, Screen Message, Log File लगायतका प्रमाणहरु सुरक्षित राख्नुहोस्।

माथि उल्लिखित सावधानीहरू अपनाई Ransomware जस्ता खतराबाट आफ्नो सूचना प्रणाली र डाटालाई सुरक्षित राख्न सम्बन्धित सबैलाई अनुरोध छ।

नोटः साइबर सुरक्षा सम्बन्धी विषयमा थप जानकारी वा सहयोग आवश्यक परेमा राष्ट्रिय साइबर सुरक्षा केन्द्र (NCSC) सँग समन्वय गर्नुहोस्।

सम्पर्कः info@ncsc.gov.np, टेलिफोनः ०१-४२११११३०, मो.नं.+९७७-९८५१४०२२८९(प्रवक्ता), +९७७-९७६३६९२२८९(सुचना अधिकारी)।