भारत में रैनसमवेयर हमले का प्रभाव।

संदर्भ

पेट्या रैनसमवेयर (Petya Ransomware) वायरस के हमले का भारत पर कोई व्यापक प्रभाव नहीं हुआ है, फिर भी सरकार उसकी निगिरानी कर रही है। सूचना एवं प्रौद्योगिकी मंत्रालय ने इस बावत विभिन्नि विभागों को चेतावनियाँ ज़ारी की हैं।

क्या है पेट्या रैनसमवेयर?

- पेट्या/नॉटपेट्या (Petya/Notpetya) रैनसमवेयर, एक दुर्भावनापूर्ण सॉफ़्टवेयर है, जो कंप्यूटर में फाइलों को लॉक कर देता है और उन फाइलों को अनलॉक करने के लिये उपयोगकर्त्ता से फिरौती की मांग करता है।
- वर्तमान साइबर हमला पेट्या रैनसमवेयर का एक रूपांतर माना जा रहा है, जो वर्ष 2016 से अस्तित्व में है।
- कैस्परस्काई (Kaspersky), जो कि एक साइबर सुरक्षा प्रदाता है, के प्रारंभिक जाँच के अनुसार, वर्तमान साइबर हमला पेट्या रैनसमवेयर का एक रूपांतर नहीं है, बल्कि एक नया रैनसमवेयर है। वह इसे नॉटपेट्या कह रही है।
- पेट्या अथवा नॉटपेट्या रैनसमवेयर, वान्नाक्राई (WannaCry) वायरस के बाद दूसरा प्रमुख वैश्विक रैनसमवेयर है, जिसका प्रभाव इतना व्यापक है। गौरतलब हो कि वान्नाक्राई वायरस ने इस वर्ष मई महीने में विश्व के 200 देशों के 3,00,000 कंप्यूटरों को प्रभावित किया था।
- वान्नाक्राई रैनसमवेयर की तरह पेट्या भी अपने आप को प्रचारित करने के साधन के रूप में बाह्य ब्लू (एक्सटर्नल ब्लू) का उपयोग करता है।
- पेट्या रैनसमवेयर न केवल फाइलों को एनक्रिप्ट (encrypt) कर देता है, बल्कि यह सम्पूर्ण डिस्क को लॉक कर देता है, जिससे यह तब तक कार्य करना बंद कर देता है, जब तक इसे हटाया नहीं जाता। यह पूरी कार्य प्रणाली को बंद कर देता है एवं उसे चालू करने के लिये बिटक्वाइनों (Bitcoins) के रूप में $ 300 फिरौती की माँग करता है।

प्रमुख घटनाक्रम

- साइबर सुरक्षा के मद्देनजर सूचना एवं प्रौद्योगिकी मंत्रालय ने स्टॉक एक्सचेंज, भारतीय विमानपत्तन प्राधिकरण, राष्ट्रीय भुगतान निगम और राष्ट्रीय क्रिटिकिल इंफॉर्मेशन इंफ्रास्ट्रक्चर प्रोटेक्शन सेंटर को चेतावनियाँ भेजी हैं। साइबर विशेषज्ञों ने इस बार बड़ी क्षति की चेतावनी दी है।
- सूचना एवं प्रौद्योगिकी मंत्रालय कैस्परस्काई, माइक्रोसॉफ्ट, मैकएफी (McAfee) एवं क्विक-हिल (Quick-Heal) जैसे सुरक्षा प्रदाताओं के साथ–साथ एशिया-प्रशांत क्षेत्र के कम्प्यूटर इमरजेंसी रिस्पाँस टीम, जिनमें हाँगकाँग, चीन और जापान शामिल हैं, के साथ भी संपर्क बनाए हुए है।

जवाहर लाल नेहरू पोर्ट ट्रस्ट

- जवाहर लाल नेहरू पोर्ट ट्रस्ट देश का सबसे बड़ा कंटेनर पोर्ट है, जिसके मुंबई टर्मिनल का परिचालन डेनिश व्यापार समूह के एपी मोलर-मेर्स्क (AP Moller-Maersk) द्वारा किया जाता है। इस कंपनी ने बम्बई स्टॉक एक्सचेंज़ को बताया है कि वह वैश्विक साइबर हमले का शिकार हुई है, जिसमें उसका गुजरात का पीपावाव बंदरगाह भी प्रभावित हुआ है।
- सरकार ने इस स्थिति से निपटने के लिये राष्ट्रीय साइबर सुरक्षा संयोजक को मुंबई स्थित जवाहर लाल नेहरू पोर्ट ट्रस्ट भेजा है, जहाँ के तीन टर्मिनलों पर इस हमले का प्रभाव हुआ है।

साइबर सुरक्षा के उपाय

- साइबर हमले से बचने के लिये यह सुनिश्चित करें कि माइक्रोसॉफ्ट विंडोज़ और सभी तृतीय पक्ष के सॉफ्टवेयर अपडेट किये गए हों। ऐसी परिस्थिति में MS17-010 बुलेटिन को तत्काल लागू करना महत्त्वपूर्ण है।
- अवांछित ई-मेल के संलग्नक को न खोलें।
- कभी भी किसी अनचाहे ई-मेल में शामिल यूआरएल पर क्लिक न करें, भले ही वे आपकी संपर्क सूची में शामिल लोगों से आए हों।
- सभी सिस्टमों पर एंटीवायरस सॉफ्टवेयर अद्यतन बनाए रखें।
- सुनिश्चित करें कि वेब ब्राउज़र सटीक नियंत्रण सामग्री के साथ पर्याप्त सुरक्षित हों।
- व्यक्तियों या संगठनों को फिरौती का भुगतान नहीं करना चाहिये, क्योंकि इसकी कोई गारंटी नहीं होती कि फाइलें रिलीज़ हो जाएंगी।
- धोखाधड़ी के ऐसे मामलों की सूचना सीईआरटी-इन(CERT-In) और विधि प्रवर्तन करने वाली एजेंसियों को दें।

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/impact-of-ransomware-attack