रैनसमवेयर हमले से बैंकों का परिचालन बाधित

प्रिलिम्स के लिये:

रैनसमवेयर, क्षेत्रीय ग्रामीण बैंक, भारतीय राष्ट्रीय भुगतान निगम, यूनिफाइड पेमेंट्स इंटरफेस, आधार-सक्षम भुगतान प्रणाली, मैलवेयर

मेन्स के लिये:

वित्तीय क्षेत्र पर रैनसमवेयर का प्रभाव, साइबर सुरक्षा उपाय, सरकारी पहलें

स्रोत: इंडियन एक्सप्रेस

चर्चा में क्यों?

हाल ही में हुए रैनसमवेयर हमले से भारत की कम-से-कम 150-200 सहकारी बैंकों के साथ क्षेत्रीय ग्रामीण बैंकों (RRB) का परिचालन बाधित हुआ है।

- भारतीय राष्ट्रीय भुगतान निगम (NPCI) द्वारा इस हमले का पता लगाया गया है। इस हमले से प्रमुख रूप से **सी-एज टेक्नोलॉजीज़ लिमिटेड** (टाटा कंसल्टेंसी सर्विसेज़ लिमिटेड (TCS) और भारतीय स्टेट बैंक (SBI) के बीच का एक संयुक्त उद्यम) द्वारा प्रदान की जाने वाली बैंकिंग सेवाएँ प्रभावित हुई हैं।

रैनसमवेयर हमले का बैंकों पर क्या प्रभाव पड़ा है?

- इन बैंकों के ग्राहक यूनिफाइड पेमेंट्स इंटरफेस (UPI) और आधार-सक्षम भुगतान प्रणाली (AePS) जैसी भुगतान प्रणालियों का उपयोग करने में असमर्थ थे।
    - इस रैनसमवेयर हमले से सी-एज टेक्नोलॉजीज़ लिमिटेड को लक्षित किये जाने के कारण इसके द्वारा सहकारी बैंकों एवं RRB को प्रदान की जाने वाली सेवाओं की गुणवत्ता प्रभावित हुई है।
- **भुगतान पारिस्थितिकी तंत्र के संदर्भ में इसके व्यापक निहितार्थ:**
    - यह हमला **प्रौद्योगिकी सेवा प्रदाताओं की भेद्यता** के साथ-साथ प्रभावी भुगतान अवसंरचना को बनाए रखने में इनकी निर्णायक भूमिका पर प्रकाश डालता है।
    - इस घटना से भविष्य में ऐसे हमलों से बचाव के क्रम में **सुदृढ़ साइबर सुरक्षा उपायों को अपनाने की आवश्यकता** को बल मिलता है।
    - इससे इस उपागम को बल मिलता है कि इस प्रकार के व्यवधानों के प्रभावों को सीमित करने के क्रम में NPCI, बैंकों एवं प्रौद्योगिकी प्रदाताओं के बीच बेहतर सहयोग हो।

नोट: AePS बैंक-नेतृत्व वाला ऐसा मॉडल है जिससे **आधार प्रमाणीकरण** के उपयोग द्वारा किसी भी बैंक के बिज़नेस कॉरेस्पॉन्डेंट के माध्यम से पॉइंट ऑफ सेल (PoS) या माइक्रो-ATM पर **ऑनलाइन इंटरऑपरेबल वित्तीय लेन-देन** की सुविधा मिलती है।

- इसे NPCI द्वारा प्रारंभ किया गया था। यह भारतीय रिज़र्व बैंक (RBI) और भारतीय बैंक संघ (IBA) की एक संयुक्त पहल है। इसका उद्देश्य गरीबों एवं हाशिये पर स्थित लोगों (विशेष रूप से ग्रामीण एवं दूर-दराज़ के क्षेत्रों से संबंधित) की बैंकिंग सेवाओं तक आसान एवं सुरक्षित पहुँच सुनिश्चित करना है।

रैनसमवेयर क्या है?

- **परिभाषा: रैनसमवेयर एक प्रकार का** मैलवेयर है, जिसके माध्यम से लक्षित डिवाइस को लॉक करने के साथ डेटा को एन्क्रिप्ट कर दिया जाता है। इसके बाद डिवाइस तक पुनः एक्सेस देने या इसे अनलॉक करने के लिये फिरौती मांगी जाती है।

- **प्रारंभिक रैनसमवेयर हमले:** प्रारंभ में किये जाने वाले रैनसमवेयर हमलों में डेटा **तक पुनः एक्सेस देने या डिवाइस को अनलॉक करने** के लिये फिरौती मांगने को प्राथमिकता दी जाती थी।
- **आधुनिक रणनीति:** हालिया रैनसमवेयर हमलों में डबल-एक्सटॉर्शन और ट्रिपल-एक्सटॉर्शन जैसी रणनीतियाँ शामिल हैं:
  - **डबल-एक्सटॉर्शन**: इसका आशय फिरौती न मिलने पर हमलावरों द्वारा चुराए गए डेटा को लीक करने की धमकी देना है।
  - **ट्रिपल-एक्सटॉर्शन**: इसका आशय हमलावरों द्वारा चुराए गए डेटा से पीड़ितों या व्यावसायिक घरानों को निशाना बनाना है।
- **रैनसमवेयर के प्रकार:**
  - **एन्क्रिप्टिंग रैनसमवेयर (क्रिप्टो रैनसमवेयर)**: इसके माध्यम से लक्षित डेटा को एन्क्रिप्ट करने के साथ इसके डिक्रिप्शन के बदले में फिरौती मांगी जाती है।
  - **नॉन-एन्क्रिप्टिंग रैनसमवेयर (स्क्रीन-लॉकिंग रैनसमवेयर):** इसके माध्यम से लक्षित डिवाइस को लॉक करने के साथ अनलॉक करने के बदले में फिरौती मांगी जाती है।
  - **रैनसमवेयर की उपश्रेणियाँ:**
    - **लीकवेयर या डॉक्सवेयर:** इसमें संवेदनशील डेटा को चुराने के साथ उसे प्रकाशित करने की धमकी देना शामिल है।
    - **मोबाइल रैनसमवेयर**: इसमें प्रायः स्क्रीन-लॉकर का उपयोग करके मोबाइल डिवाइस को प्रभावित करना शामिल है।
    - **वाइपर**: इसमें डेटा को नष्ट करने की धमकी देना शामिल है। कभी-कभी फिरौती देने पर भी डेटा को नष्ट कर दिया जाता है।
    - **स्केयरवेयर**: इसमें भुगतान हेतु दबाव बनाने के क्रम में भययुक्त माहौल बनाना शामिल है।
- **साइबर हमले के रूप में रैनसमवेयर:**
  - **वित्तीय प्रभाव**: रैनसमवेयर हमलों से लक्षित निकायों को लाखों डॉलर का नुकसान हो सकता है।
    - IBM (इंटरनेशनल बिज़नेस मशीन कॉर्पोरेशन) की एक रिपोर्ट के अनुसार वित्तीय वर्ष 2024 में **डेटा उल्लंघन की औसत लागत 19.5 करोड़ रुपए (USD 2.35 मिलियन) के उच्चतम स्तर (** जो वर्ष 2023 की तुलना में लगभग 7% अधिक है) पर पहुँच गई, जिसमें स्थानीय औद्योगिक क्षेत्र सबसे अधिक प्रभावित हुए।
    - रैनसमवेयर से पीड़ित, फिरौती भुगतान के बारे में बताने से बचते हैं।
  - **हमलों की तीव्रता**: हैकर्स को नेटवर्क तक पहुँच मिल जाने के बाद **चार दिनों से भी कम समय** में रैनसमवेयर हमला कर दिया जाता है जिससे संगठनों को इसका पता लगाने एवं **प्रतिक्रिया देने के लिये बहुत कम समय मिलता** है।
- **रैनसमवेयर की प्रतिक्रिया में उठाए जाने वाले कदम:**
  - इसके प्रसार को रोकने हेतु लक्षित **डिवाइस को नेटवर्क से पृथक करना**।
  - किसी भी सक्रिय निगरानी प्लेटफॉर्म के माध्यम से **किसी भी जोखिम की जाँच करके इस हमले** की पहचान करना और एन्क्रिप्टेड फाइलों एवं फिरौती की सूचनाओं को स्कैन करके रैनसमवेयर की पहचान करना।
  - संबंधित नेटवर्क को हमले से बचाने के साथ उसके पुनर्नवीनीकरण **को प्राथमिकता देना**।
    - यदि बैकअप उपलब्ध है तो बैकअप के माध्यम से संबंधित प्रणाली को पुनर्स्थापित करना या **डिक्रिप्शन विकल्पों हेतु प्रयास करना**।

रैनसमवेयर किसी नेटवर्क को किस प्रकार संक्रमित करता है?

- **फिशिंग**: इसमें [सोशल इंजीनियरिंग ट्रिक्स] के उपयोग द्वारा फेक लिंक के माध्यम से रैनसमवेयर डाउनलोड करवाने का प्रयास किया जाता है।
  - सोशल इंजीनियरिंग ट्रिक्स द्वारा उपयोगकर्त्ताओं को सुरक्षा संबंधी गलतियाँ करने या संवेदनशील जानकारी प्रकट करने के लिये प्रेरित किया जाता है।
- **वल्नरेबिलिटी का लाभ उठाना:** इसके तहत रैनसमवेयर को इंजेक्ट करने के क्रम में मौजूदा या [ज़ीरो-डे वल्नरेबिलिटी] का उपयोग करना शामिल है।
- **क्रेडेंशियल थेफ्ट (Credential Theft)**: इसमें रैनसमवेयर को इंजेक्ट करने के क्रम में अधिकृत उपयोगकर्त्ता क्रेडेंशियल की चोरी करना शामिल है।
- **अन्य मैलवेयर**: रैनसमवेयर के प्रसार के लिये अन्य मैलवेयर (जैसे- [ट्रोजन]) का उपयोग किया जाता है।
- **ड्राइव-बाय डाउनलोड**: इसका आशय कॉम्प्रोमाइज़्ड वेबसाइटों के माध्यम से किसी डिवाइस को संक्रमित करना है।
- **सेवा के रूप में रैनसमवेयर (RaaS):** इसका तात्पर्य साइबर अपराधियों द्वारा फिरौती के हिस्से के बदले में दूसरों द्वारा विकसित रैनसमवेयर का उपयोग करना है।

उल्लेखनीय रैनसमवेयर वैरिएंट

- [अकीरा रैनसमवेयर]
- [LockBit रैनसमवेयर]
- **क्रिप्टो लॉकर:** इसे वर्ष 2013 से रैनसमवेयर के आधुनिक युग की शुरुआत करने का श्रेय दिया जाता है।
- **वानाक्राई:** यह एक प्रकार का क्रिप्टोवर्म है जिसके द्वारा वर्ष 2017 में 150 देशों के 200,000 से अधिक कंप्यूटरों को प्रभावित किया गया था।
- **पेट्या और नॉटपेट्या:** इसके द्वारा फाइल सिस्टम टेबल को एन्क्रिप्ट किया जाता है, जिससे कंप्यूटर बूट करने में असमर्थ हो जाते हैं।
- **रयूक:** इसके माध्यम से उच्च-मूल्य वाले लक्ष्यों के खिलाफ बिग-गेम रैनसमवेयर हमलों को लोकप्रिय बनाया गया।
- **डार्कसाइड:** यह वर्ष 2021 के कोलोनियल पाइपलाइन हमले के लिये ज़िम्मेदार है।
- **लॉकी:** इसके तहत डिवाइस को प्रभावित करने के क्रम में ईमेल अटैचमेंट में मैक्रोज़ का उपयोग किया जाता है।
- **रेविल:** इसे बिग-गेम हन्टिंग और डबल-एक्सटॉर्शन अटैक के लिये जाना जाता है।
- **कॉन्टी:** इसके तहत डबल-एक्सटॉर्शन रणनीति के उपयोग के माध्यम से RaaS स्कीम को ऑपरेट किया जाना शामिल है।

भारत में रैनसमवेयर हमलों से बचाव हेतु क्या कानून हैं?

- रैनसमवेयर हमले **भारतीय दंड संहिता, 1860** और **सूचना प्रौद्योगिकी (IT) अधिनियम, 2000** के तहत विभिन्न प्रकार के अपराध की श्रेणी में शामिल हैं।
    - IT अधिनियम की विभिन्न धाराएँ **इससे संबंधित हैं: धारा 43 और 66 (कंप्यूटर/सिस्टम को क्षति पहुँचाना), धारा 65 (कंप्यूटर स्रोत पर दस्तावेज़ों में हेरफेर करना) और धारा 66D (पहचान बदलकर धोखाधड़ी करना)।** इसके अतिरिक्त संवेदनशील व्यक्तिगत डेटा रखने वाले कॉर्पोरेट निकायों पर IT नियमों के तहत उचित सुरक्षा प्राथमिकताओं को अपनाने का दायित्व है।
    - IT अधिनियम के तहत रैनसमवेयर हमलों के लिये तीन से सात वर्ष तक के कारावास के साथ एक करोड़ रुपए तक के जुर्माने का प्रावधान है।
- **भारत के राष्ट्रीय साइबर सुरक्षा समन्वयक (NCSC)** संगठन के अंतर्गत एक विशेष इकाई के रूप में रैनसमवेयर टास्क फोर्स (RTF), रैनसमवेयर हमलों के पीड़ितों के लिये एक केंद्रीय संपर्क बिंदु के रूप में कार्य करने के साथ इस संदर्भ में जाँच, पुनर्प्राप्ति एवं रोकथाम प्रयासों में सहायता प्रदान करती है।
- **भारतीय रिज़र्व बैंक** द्वारा जारी भारतीय बैंकिंग क्षेत्र के लिये **साइबर सुरक्षा फ्रेमवर्क, 2018 के माध्यम से बैंकों** और वित्तीय संस्थानों को रैनसमवेयर हमलों सहित साइबर खतरों से बचाने के लिये विशिष्ट दिशा-निर्देश दिये गए हैं।
    - इसके तहत बैंकों को बहु-स्तरीय प्रमाणीकरण, एन्क्रिप्शन और नियमित सुरक्षा ऑडिट जैसे मज़बूत साइबर सुरक्षा उपायों को लागू करने का निर्देश दिया गया।

//

आगे की राह

- **साइबर सुरक्षा का उन्नयन करना: बैंकों और प्रौद्योगिकी सेवा प्रदाताओं को एंडपॉइंट सुरक्षा, नेटवर्क सुरक्षा, डेटा बैकअप तथा कर्मचारी प्रशिक्षण सहित मज़बूत साइबर सुरक्षा उपायों को लागू करना चाहिये।**
    - साइबर खतरों का पता लगाने के साथ इसकी रोकथाम पर बल दिये जाने के कारण वर्ष 2022 व 2023 के बीच रैनसमवेयर इन्फेक्शन में 11.5% की कमी आई है।
    - **बैंकों और वित्तीय संस्थानों के बीच साइबर खतरों से संबंधित** खुफिया जानकारी साझा करने के लिये एक केंद्रीकृत प्लेटफॉर्म स्थापित करना चाहिये।
- **डेटा बैकअप और रिकवरी: ऑफलाइन बैकअप सहित डेटा बैकअप और रिकवरी प्रक्रियाओं को मज़बूत बनाना चाहिये।**

- **उन्नत सुरक्षा मानक:** थर्ड पार्टी वेंडर्स एवं भागीदारों के सुरक्षा मूल्यांकन को मज़बूत बनाना चाहिये। इसके साथ ही साइबर हमलों के प्रभाव को कम करने के लिये हमलों की प्रतिक्रिया क्षमताओं में सुधार करना चाहिये।
    - सुरक्षा के प्रति प्रतिबद्धता प्रदर्शित करने के क्रम में प्रासंगिक **साइबर सुरक्षा प्रमाण-पत्र** को प्राप्त करना आवश्यक बनाना चाहिये।

दृष्टि मेन्स प्रश्न:

प्रश्न. बैंकिंग पारिस्थितिकी तंत्र पर रैनसमवेयर हमले के प्रभावों का विश्लेषण कीजिये और इन जोखिमों को कम करने के लिये संगठन क्या उपाय लागू कर सकते हैं?

UPSC सिविल सेवा परीक्षा, विगत वर्ष के प्रश्न

??????????:

प्रश्न. 'वानाक्राई, पेट्या और इटरनलब्लू' जो हाल ही में समाचारों में उल्लिखित थे, निम्नलिखित में से किससे संबंधित हैं? (2018)

(a) एक्सोप्लैनेट्स
(b) क्रिप्टोकरेंसी
(c) साइबर आक्रमण
(d) लघु उपग्रह

उत्तर: (c)

प्रश्न. भारत में साइबर सुरक्षा घटनाओं पर रिपोर्ट करना निम्नलिखित में से किसके/किनके लिये विधितः अधिदेशात्मक है? (2017)

1. सेवा प्रदाता (सर्विस प्रोवाइडर)
2. डेटा सेंटर
3. कॉर्पोरेट निकाय (बॉडी कॉर्पोरेट)

नीचे दिये गए कूट का प्रयोग कर सही उत्तर चुनिये:

(a) केवल 1
(b) केवल 1 और 2
(c) केवल 3
(d) 1, 2 और 3

उत्तर: (d)

?????:

प्रश्न. साइबर सुरक्षा के विभिन्न तत्त्व क्या हैं? साइबर सुरक्षा की चुनौतियों को ध्यान में रखते हुए समीक्षा कीजिये कि भारत ने किस हद तक एक व्यापक राष्ट्रीय साइबर सुरक्षा रणनीति सफलतापूर्वक विकसित की है। (2022)

प्रश्न. साइबर आक्रमण के संभावित खतरों की एवं रोकने के लिये सुरक्षा ढाँचे की विवेचना कीजिये।(2017)

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/ransomware-attack-disrupts-bank-operations