रैनसमवेयर हमले से बैंकों का परचिालन बाधति

प्रलिमि्स के लयि:

रैनसमवेयर, क्षेत्रीय ग्रामीण बैंक, भारतीय राष्ट्रीय भुगतान नगिम, यूनफिाइड पेमेंट्स इंटरफ़ेस, आधार-सक्षम भुगतान प्रणाली, मैलवेयर

मेन्स के लयि:

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

स्रोत: इंडयिन 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 परचिालन बाधति हुआ है।

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

रैनसमवेयर हमले का बैंकों पर क्या प्रभाव पड़ा है?

- इन बैंकों के ग्राहक यूनफिाइड पेमेंट्स इंटरफेस (UPI) और आधार-सक्षम भुगतान प्रणाली (AePS) जैसी भुगतान प्रणालयिों का उपयोग करने मैं असमर्थ थे।
  - इस रैनसमवेयर हमले से सी-एज टेक्नोलॉजीज़ लमिटिेड को लक्षति कयि जाने के कारण इसके द्वारा सहकारी बैंकों एवं RRB को प्रदान की जाने वाली सेवाओं की गुणवत्ता प्रभावति हुई है।
- **भुगतान पारस्थितिकी तंत्र के संदर्भ में इसके व्यापक नहितिार्थ:**
  - यह हमला **प्रौद्योगकिी सेवा प्रदाताओं की भेद्यता** के साथ-साथ प्रभावी भुगतान अवसंरचना को बनाए रखने में इनकी नर्णिायक भूमकिा पर प्रकाश डालता है।
  - इस घटना से भवषि्य में ऐसे हमलों से बचाव के क्रम में **सुदृढ़** साइबर सुरक्षा उपायों **को अपनाने की आवश्यकता** को बल मलिता है।
  - इससे इस उपागम को बल मलिता है कि इस प्रकार के व्यवधानों के प्रभावों को सीमति करने के क्रम में NPCI, बैंकों एवं प्रौद्योगकिी प्रदाताओं के बीच बेहतर सहयोग हो।

नोट: AePS बैंक-नेतृत्व वाला ऐसा मॉडल है जसिसे **आधार प्रमाणीकरण** के उपयोग द्वारा कसिी भी बैंक के बज़िनेस कॉरेस्पॉन्डेंट के माध्यम से पॉइंट ऑफ सेल (PoS) या माइक्रो-ATM पर **ऑनलाइन इंटरऑपरेबल वत्तिीय लेन-देन** की सुवधिा मलिती है।

- इसे NPCI द्वारा प्रारंभ कयि गया था। यह भारतीय रज़िर्व बैंक (RBI) और भारतीय बैंक संघ (IBA) की एक संयुक्त पहल है। इसका उद्देश्य गरीबों एवं हाशयि पर स्थति लोगों (वशिेष रूप से ग्रामीण एवं दूर-दराज़ के क्षेत्रों से संबंधति) की बैंकगि सेवाओं तक आसान एवं सुरक्षति पहुँच सुनश्चिति करना है।

रैनसमवेयर क्या है?

- **परभिाषा: रैनसमवेयर एक प्रकार का** मैलवेयर है, जसिके माध्यम से लक्षति डवािइस को लॉक करने के साथ डेटा को एन्क्रप्टि कर दयि जाता है। इसके बाद डवािइस तक पुनः एक्सेस देने या इसे अनलॉक करने के लयि फरिौती मांगी जाती है।

- **प्रारंभकि रैनसमवेयर हमले:** प्रारंभ में कयि जाने वाले रैनसमवेयर हमलों में डेटा **तक पुनः एक्सेस देने या डविाइस को अनलॉक करने** के लयि फरिौती मांगने को प्राथमकिता दी जाती थी।
- **आधुनकि रणनीति:** हालयिा रैनसमवेयर हमलों में डबल-एक्सटॉर्शन और ट्रपिल-एक्सटॉर्शन जैसी रणनीतयिाँ शामलि हैं:
  - **डबल-एक्सटॉर्शन**: इसका आशय फरिौती न मलिने पर हमलावरों द्वारा चुराए गए डेटा को लीक करने की धमकी देना है।
  - **ट्रपिल-एक्सटॉर्शन**: इसका आशय हमलावरों द्वारा चुराए गए डेटा से पीड़तिों या व्यावसायकि घरानों को नशिाना बनाना है।
- **रैनसमवेयर के प्रकार:**
  - **एन्क्रप्टिगि रैनसमवेयर (क्रप्टिो रैनसमवेयर)**: इसके माध्यम से लक्षति डेटा को एन्क्रप्टि करने के साथ इसके डक्रिप्शिन के बदले में फरिौती मांगी जाती है।
  - **नॉन-एन्क्रप्टिगि रैनसमवेयर (स्क्रीन-लॉकगि रैनसमवेयर):** इसके माध्यम से लक्षति डविाइस को लॉक करने के साथ अनलॉक करने के बदले में फरिौती मांगी जाती है।
  - **रैनसमवेयर की उपश्रेणयिाँ:**
    - **लीकवेयर या डॉक्सवेयर:** इसमें संवेदनशील डेटा को चुराने के साथ उसे प्रकाशति करने की धमकी देना शामलि है।
    - **मोबाइल रैनसमवेयर**: इसमें प्रायः स्क्रीन-लॉकर का उपयोग करके मोबाइल डविाइस को प्रभावति करना शामलि है।
    - **वाइपर**: इसमें डेटा को नष्ट करने की धमकी देना शामलि है। कभी-कभी फरिौती देने पर भी डेटा को नष्ट कर दयि जाता है।
    - **स्केयरवेयर**: इसमें भुगतान हेतु दबाव बनाने के क्रम में भययुक्त माहौल बनाना शामलि है।
- **साइबर हमले के रूप में रैनसमवेयर:**
  - **वत्तिीय प्रभाव**: रैनसमवेयर हमलों से लक्षति नकियों को लाखों डॉलर का नुकसान हो सकता है।
    - IBM (इंटरनेशनल बज़िनेस मशीन कॉर्पोरेशन) की एक रपिोर्ट के अनुसार वत्तिीय वर्ष 2024 में**डेटा उल्लंघन की औसत लागत 19.5 करोड़ रुपए (USD 2.35 मलियिन) के उच्चतम स्तर (** जो वर्ष 2023 की तुलना में लगभग 7% अधकि है) पर पहुँच गई, जसिमें स्थानीय औद्योगकि क्षेत्र सबसे अधकि प्रभावति हुए।
    - रैनसमवेयर से पीड़ति, फरिौती भुगतान के बारे में बताने से बचते हैं।
  - **हमलों की तीव्रता**: हैकर्स को नेटवर्क तक पहुँच मलि जाने के बाद **चार दनिों से भी कम समय** में रैनसमवेयर हमला कर दयि जाता है जसिसे संगठनों को इसका पता लगाने एवं **प्रतक्रियिा देने के लयि बहुत कम समय मलिता** है।
- **रैनसमवेयर की प्रतक्रियिा में उठाए जाने वाले कदम:**
  - इसके प्रसार को रोकने हेतु लक्षति **डविाइस को नेटवर्क से पृथक करना**।
  - कसिी भी सक्रयि नगिरानी प्लेटफॉर्म के माध्यम से **कसिी भी जोखमि की जाँच करके इस हमले** की पहचान करना और एन्क्रप्टिेड फाइलों एवं फरिौती की सूचनाओं को स्कैन करके रैनसमवेयर की पहचान करना।
  - संबंधति नेटवर्क को हमले से बचाने के साथ उसके पुनर्नवीनीकरण **को प्राथमकिता देना**।
    - यदि बैकअप उपलब्ध है तो बैकअप के माध्यम से संबंधति प्रणाली को पुनर्स्थापति करना या**डक्रिप्शिन वकिल्पों हेतु प्रयास करना**।

रैनसमवेयर कसिी नेटवर्क को कसि प्रकार संक्रमति करता है?

- **फशिगि**: इसमें [सोशल इंजीनयिरगि ट्रक्सि](#) के उपयोग द्वारा फेक लकि के माध्यम से रैनसमवेयर डाउनलोड करवाने का प्रयास कयि जाता है।
  - सोशल इंजीनयिरगि ट्रक्सि द्वारा उपयोगकर्त्ताओं को सुरक्षा संबंधी गलतयिाँ करने या संवेदनशील जानकारी प्रकट करने के लयि प्रेरति कयि जाता है।
- **वल्नरेबलिटिी का लाभ उठाना:** इसके तहत रैनसमवेयर को इंजेक्ट करने के क्रम में मौजूदा या [ज़ीरो-डे वल्नरेबलिटिी](#) का उपयोग करना शामलि है।
- **क्रेडेंशयिल थेफ्ट (Credential Theft)**: इसमें रैनसमवेयर को इंजेक्ट करने के क्रम में अधकिृत उपयोगकर्त्ता क्रेडेंशयिल की चोरी करना शामलि है।
- **अन्य मैलवेयर**: रैनसमवेयर के प्रसार के लयि अन्य मैलवेयर (जैसे- [ट्रोजन](#)) का उपयोग कयि जाता है।
- **ड्राइव-बाय डाउनलोड**: इसका आशय कॉम्प्रोमाइज्ड वेबसाइटों के माध्यम से कसिी डविाइस को संक्रमति करना है।
- **सेवा के रूप में रैनसमवेयर (RaaS):** इसका तात्पर्य साइबर अपराधयिों द्वारा फरिौती के हस्सि के बदले में दूसरों द्वारा वकिसति रैनसमवेयर का उपयोग करना है।

उल्लेखनीय रैनसमवेयर वैरएिंट

- [अकीरा रैनसमवेयर](#)
- [LockBit रैनसमवेयर](#)
- **क्रप्टिो लॉकर:** इसे वर्ष 2013 से रैनसमवेयर के आधुनकि युग की शुरुआत करने का श्रेय दयि जाता है।
- **वानाक्राई:** यह एक प्रकार का क्रप्टिोवर्म है जसिके द्वारा वर्ष 2017 में 150 देशों के 200,000 से अधकि कंप्यूटरों को प्रभावति कयि गया था।
- **पेट्या और नॉटपेट्या:** इसके द्वारा फाइल सस्टिम टेबल को एन्क्रप्टि कयि जाता है, जसिसे कंप्यूटर बूट करने में असमर्थ हो जाते हैं।
- **रयूक:** इसके माध्यम से उच्च-मूल्य वाले लक्ष्यों के खलिाफ बगि-गेम रैनसमवेयर हमलों को लोकप्रयि बनाया गया।
- **डार्कसाइड:** यह वर्ष 2021 के कोलोनयिल पाइपलाइन हमले के लयि ज़म्मिेदार है।
- **लॉकी:** इसके तहत डविाइस को प्रभावति करने के क्रम में ईमेल अटैचमेंट में मैक्रोज़ का उपयोग कयि जाता है।
- **रेवलि:** इसे बगि-गेम हन्टगि और डबल-एक्सटॉर्शन अटैक के लयि जाना जाता है।
- **कॉन्टी:** इसके तहत डबल-एक्सटॉर्शन रणनीति के उपयोग के माध्यम से RaaS स्कीम को ऑपरेट कयि जाना शामलि 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)