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 रैनसमवेयर हमले ने भारत में कम-से-कम 150-200 सहकारी बैंकों और क्षेत्रीय ग्रामीण बैंकों (RRB) के परिचालन को गंभीर रूप से बाधित कर दिया।

- भारतीय राष्ट्रीय भुगतान निगम (NPCI) ने इस हमले की पहचान की है, जिसने मुख्य रूप से **टाटा कंसल्टेंसी सर्विसिज़ लिमिटेड (TCS)** और भारतीय स्टेट बैंक (SBI) के बीच एक संयुक्त उद्यम **सी-एज टेक्नोलॉजीज़ लिमिटेड** द्वारा सेवा प्रदान करने वाले बैंकों को प्रभावित किया है।

रैनसमवेयर हमले का बैंकों पर क्या प्रभाव पड़ा है?

- रैनसमवेयर हमले ने सी-एज टेक्नोलॉजीज़ लिमिटेड को निशाना बनाया, जिससे सहकारी बैंकों और RRB को सेवाएँ प्रदान करने की उनकी क्षमता प्रभावित हुई।
  - प्रभावित बैंकों के ग्राहक यूनिफाइड पेमेंट्स इंटरफेस (UPI) और आधार-सक्षम भुगतान प्रणाली (AePS) सहित भुगतान प्रणालियों तक पहुँचने में असमर्थ थे।
  - कुछ RRB, अपने प्रायोजक बैंकों के आधार पर कार्य करना जारी रखते हैं क्योंकि वे विभिन्न प्रौद्योगिकी सेवा प्रदाताओं का उपयोग करते हैं।
- **भुगतान पारिस्थितिकी तंत्र के व्यापक निहितार्थ:**
  - यह हमला **प्रौद्योगिकी सेवा प्रदाताओं की भेद्यता** और भुगतान अवसंरचना को बनाए रखने में उनकी महत्त्वपूर्ण भूमिका को उज़ागर करता है।
  - यह घटना भविष्य में ऐसे हमलों से बचाव के लिये **सुदृढ़** साइबर सुरक्षा उपायों **की आवश्यकता** को रेखांकित करती है।
  - इस प्रकार के व्यवधानों के प्रभावों को कम करने के लिये NPCI, बैंकों और प्रौद्योगिकी प्रदाताओं के बीच सहयोग महत्त्वपूर्ण है।

नोट: AePS एक बैंक-नेतृत्व वाला मॉडल है जो **आधार प्रामाणीकरण** का उपयोग करके किसी भी बैंक के बिज़नेस कॉरेस्पॉन्डेंट के माध्यम से पॉइंट ऑफ सेल (PoS) या माइक्रो-ATM पर **ऑनलाइन इंटरऑपरेबल वित्तीय लेन-देन** की अनुमति देता है।

- इसे NPCI द्वारा प्रारंभ किया गया था, जो भारतीय रिज़र्व बैंक (RBI) और भारतीय बैंक संघ (IBA) की एक संयुक्त पहल है, जिसका उद्देश्य गरीबों तथा हाशिये पर पड़े लोगों, मूलतः ग्रामीण एवं दूर-दराज़ के क्षेत्रों में बैंकिंग सेवाओं तक आसान और सुरक्षित पहुँच प्रदान करना है।

रैनसमवेयर क्या है?

- **परिभाषा: रैनसमवेयर एक प्रकार का** मैलवेयर है, जो पीड़ित के डेटा को एन्क्रिप्ट करता है या उनके डिवाइस को लॉक कर देता है, जिसके

परिणामस्वरूप एक्सेस वापस देने या फिर डिक्रिप्शन कुंजी के लिये फिरौती मांगी जाती है।

- **प्रारंभिक हमले:** प्रारंभ में रैनसमवेयर हमले **डेटा को एन्क्रिप्ट करने और डिक्रिप्शन कुंजी** के लिये फिरौती मांगने पर केंद्रित थे।
- **आधुनिक रणनीति:** हालिया रैनसमवेयर हमलों में डबल-एक्सटॉर्शन और ट्रिपल-एक्सटॉर्शन रणनीति शामिल हैं:
  - **डबल-एक्सटॉर्शन**: हमलावर फिरौती न मिलने पर चुराए गए डेटा को ऑनलाइन लीक करने की धमकी देते हैं।
  - **ट्रिपल-एक्सटॉर्शन**: हमलावर पीड़ितों या व्यावसायिक भागीदारों को निशाना बनाने के लिये चुराए गए डेटा का उपयोग करते हैं।
- **रैनसमवेयर के प्रकार:**
  - **एन्क्रिप्टिंग रैनसमवेयर (क्रिप्टो रैनसमवेयर)**: पीड़ित के डेटा को एन्क्रिप्ट करता है, जिसके द्वारा डिक्रिप्शन कुंजी के लिये फिरौती की मांग की जाती है।
  - **नॉन-एन्क्रिप्टिंग रैनसमवेयर (स्क्रीन-लॉकिंग रैनसमवेयर):** पीड़ित के पूरे डिवाइस को लॉक कर देता है, स्क्रीन पर फिरौती की मांग की जाती है।
  - **रैंसमवेयर की उपश्रेणियों में शामिल हैं:**
    - **लीकवेयर या डॉक्सवेयर:** संवेदनशील डेटा चुराता है और उसे प्रकाशित करने की धमकी देता है।
    - **मोबाइल रैनसमवेयर**: प्रायः स्क्रीन-लॉकर का उपयोग करके मोबाइल डिवाइस को प्रभावित करता है।
    - **वाइपर**: डेटा को नष्ट करने की धमकी देता है, कभी-कभी फिरौती का भुगतान करने पर भी ऐसा देखा जाता है।
    - **स्केयरवेयर**: भुगतान के लिये दबाव डालने के लिये भय का माहौल बनता है, जिसे कभी-कभी वैध अलर्ट के रूप में प्रस्तुत करता है।
- **साइबर हमले के रूप में रैनसमवेयर:**
  - **वित्तीय प्रभाव**: रैनसमवेयर हमलों से संगठनों को लाखों डॉलर का नुकसान हो सकता है।
    - IBM (इंटरनेशनल बिज़िनेस मशीन कॉर्पोरेशन) की एक रिपोर्ट से पता चला है कि वित्तीय वर्ष 2024 में **डेटा उल्लंघन की औसत लागत 19.5 करोड़ रुपए (USD 2.35 मिलियन) के उच्चतम स्तर** को स्पर्श कर गई, जो वर्ष 2023 की तुलना में लगभग 7% अधिक है, जिसमें स्थानीय औद्योगिक क्षेत्र सबसे अधिक प्रभावित है।
    - रैंसमवेयर पीड़ित और वार्ताकार (Negotiator) फिरौती भुगतान का खुलासा करने से कतराते हैं।
  - **हमलों की गति:** एक बार जब हैकर्स को नेटवर्क तक पहुँच मिल जाती है, तो वे **चार दिनों से भी कम समय** में रैनसमवेयर तैनात कर सकते हैं, जिससे संगठनों को पता लगाने और **प्रतिक्रिया देने के लिये बहुत कम समय मिलता** है।
- **रैनसमवेयर का जवाब देने के लिये उठाए गए कदम:**
  - संक्रमण को रोकने हेतु **संक्रमित डिवाइस को नेटवर्क से पृथक करना** । संक्रमण के प्रसार को रोकने के लिये सभी संदिग्ध व्यवहार करने वाले डिवाइस को नेटवर्क से डिस्कनेक्ट करना।
  - किसी भी सक्रिय निगरानी प्लेटफॉर्म के माध्यम से **किसी भी अलर्ट की जाँच करके प्रवेश बिंदु** की पहचान करना और एन्क्रिप्टेड फाइलों एवं फिरौती की सूचनाओं को स्कैन करके रैनसमवेयर की पहचान करना।
  - सबसे महत्त्वपूर्ण सिस्टम को पहले पुनर्स्थापित करके और उसके बाद नेटवर्क से हमले को खत्म करके **सिस्टम की बहाली को प्राथमिकता देना**।
    - यदि बैकअप उपलब्ध है, तो बैकअप से सिस्टम को पुनर्स्थापित करना। **अन्यथा, डिक्रिप्शन विकल्पों के लिये प्रयास करना**।

रैनसमवेयर सिस्टम को कैसे संक्रमित करता है?

- **फिशिंग**: यह एक प्रकार का साइबर हमला है, जो दुर्भावनापूर्ण अनुलग्नकों (Malicious Attachments) या लिंक के माध्यम से पीड़ितों को रैनसमवेयर डाउनलोड करने हेतु धोखा देने के लिये **सोशल इंजीनियरिंग ट्रिक्स** का उपयोग करता है।
  - सोशल इंजीनियरिंग मनोवैज्ञानिक छल का उपयोग है, जो उपयोगकर्त्ताओं को सुरक्षा संबंधी गलतियाँ करने या संवेदनशील जानकारी प्रकट करने के लिये प्रेरित करता है।
- **कमज़ोरियों का दोहन:** रैनसमवेयर को इंजेक्ट करने के लिये मौजूदा या **ज़ीरो-डे वल्नरेबिलिटी** का उपयोग करता है।
- **क्रेडेंशियल की चोरी (Credential Theft)**: रैनसमवेयर को तैनात करने के लिये अधिकृत उपयोगकर्त्ता क्रेडेंशियल की चोरी करता है।
- **अन्य मैलवेयर**: रैनसमवेयर के प्रसार के लिये अन्य मैलवेयर (जैसे- **ट्रोजन**) का उपयोग करना।
- **ड्राइव-बाय डाउनलोड**: कॉम्प्रोमाइज्ड वेबसाइटों के माध्यम से उपकरणों को संक्रमित करता है।
- **सेवा के रूप में रैनसमवेयर (RaaS):** साइबर अपराधियों को फिरौती के एक भाग के बदले में दूसरों द्वारा विकसित रैनसमवेयर का उपयोग करने की अनुमति देता है।

उल्लेखनीय रैनसमवेयर वैरिएंट

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

- **कॉन्ट्री:** डबल-एक्सटॉर्शन रणनीति का उपयोग करके एक RaaS योजना संचालित करता है।

HOW RANSOMWARE WORKS

Malicious code blocks access to the data in your computer

You receive an infected file (typically attached to an email or a URL); if you open it, you've let malicious code into your computer

Encryption key locks all your data

Without the key, all the files on your computer are locked

Command and control server

In a matter of minutes, your files are out of reach

When you try to open a file, a message appears demanding a ransom

Payment in cryptocurrency bitcoin helps hackers cover their tracks

If you don't pay

- Your encrypted files are lost

If you pay

- You send the ransom money to an anonymous recipient hiding in the 'Darknet'
- Normally, you get the key to the data in an hour or so

WHAT IS RANSOMWARE

- The malware shutting down computers worldwide is **known as WannaCry** and variants of that name
- This type of malware is **called ransomware as it first scrambles a victim's files and then demands a payment** to unscramble them

HOW DOES IT WORK

- WannaCry seems to be deployed via a worm — a programme that spread by itself between computers
- Once malware is inside an organisation, it will find vulnerable machines and infect them too
- Infections reported in 150 countries, including Russia and China. In UK, hospital systems badly hit

HOW THE HACKERS STRUCK

- The ransomware exploits a weakness in Microsoft Windows systems that was identified by the US National Security Agency and given the name 'EternalBlue'
- But NSA's code was among a cache stolen by a hackers' group known as The Shadow Brokers, who then attempted to sell it in an online auction
- The hackers' group later made the tools freely available in April, saying it was a "protest" against US President Donald Tump
- Microsoft had by then already released a software upgrade fixing the issue
- But not all users were prompt in installing the upgrades

How They FELL FOR IT

- Cyber extortionists tricked victims into opening malicious attachments to spam emails that appeared to contain legitimate files
- The ransomware encrypted data on the computers, demanding payments of $300 to $600 via the digital currency bitcoin to restore access

GOVT AGENCIES/COMPANIES AFFECTED GLOBALLY

- Britain's National Health Service (NHS)
- Russian interior ministry (about 1,000 computers)
- Spain's communications giant Telefonica
- Spain's power firm Iberdrola
- FedEx in the US
- Japanese carmaker Nissan's plant in England
- German rail operator Deutsche Bahn
- French automaker Renault halted production at several sites in Europe

GLOBAL IMPACT

- A cyber security firm said it had seen 2,00,000 cases of the Wanna Cry attack
- Asian nations also hit hard by the ransomware

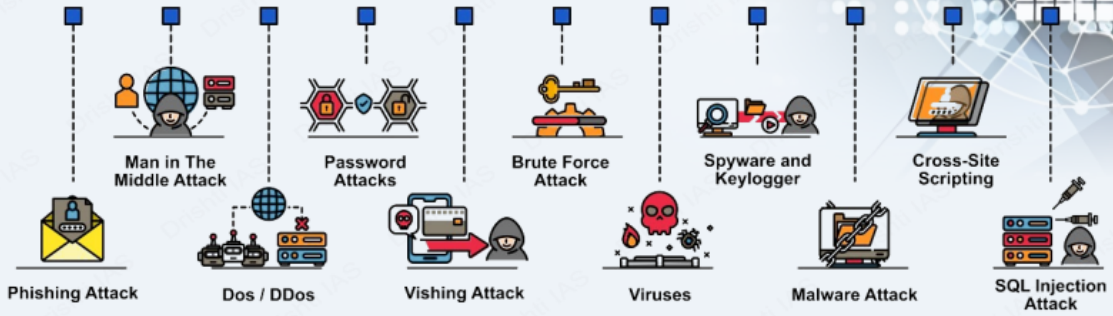
भारत में रैनसमवेयर हमलों से बचाव के लयि क्या कानून हैं?

- रैनसमवेयर हमले भारतीय दंड संहति 1860 और सूचना प्रौद्योगकिी (IT) अधनियिम 2000 के तहत वभिन्नि अपराध हैं।
    - IT अधनियिम में **प्रासंगकि प्रावधान शामलि हैं: धारा 43 और 66 (कंप्यूटर/ससि्टम को नुकसान पहुँचाना), धारा 65 (कंप्यूटर स्रोत दस्तावेज़ों के साथ छेड़छाड़ करना) और धारा 66D (पहचान बदलकर धोखाधड़ी करना)।** इसके अतरिक्ति, संवेदनशील व्यक्तगित डेटा रखने वाले कॉर्पोरेट नकिायों का IT नयिमों के तहत उचति सुरक्षा प्रथाओं को लागू करने का दायत्वि है।
    - IT अधनियिम के तहत रैनसमवेयर हमलों के लयि तीन वर्ष से सात वर्ष तक की कैद और एक करोड़ रुपए तक के जुर्माने का प्रावधान है।
- **रैनसमवेयर टास्क फोर्स (RTF), भारत के राष्ट्रीय साइबर सुरक्षा समन्वयक (NCSC)** संगठन के अंतर्गत एक वशिष इकाई है, जो रैनसमवेयर हमलों के पीड़तिों के लयि एक केंद्रीय संपर्क बदिु के रूप में कार्य करती है तथा जाँच, पुनर्प्राप्तएिवं रोकथाम प्रयासों में सहायता प्रदान करती है।
- भारतीय रज़िर्व बैंक द्वारा जारी भारतीय बैंकगि क्षेत्र के लयि **साइबर सुरक्षा फ्रेमवर्क, 2018 बैंकों** और वत्तिीय संस्थानों को रैनसमवेयर हमलों सहति साइबर खतरों से बचाने के लयि वशिष्टि दशिा-नर्दिेश प्रदान करता है।
    - इसमें बैंकों को बहु-कारक प्रामाणीकरण, एन्क्रप्शिन और नयिमति सुरक्षा ऑडटि जैसे मज़बूत साइबर सुरक्षा उपायों को लागू करने का नर्दिेश दयिा गया है।

साइबर सुरक्षा

साइबर सुरक्षा, साइबर हमलों को रोकने या उनके प्रभाव को कम करने के लिये किसी भी तकनीक, उपाय या अभ्यास को संदर्भित करती है।

CYBER SECURITY ATTACKS



NCRB की "भारत में अपराध" रिपोर्ट, 2022 के अनुसार, वर्ष 2021 के बाद से भारत में साइबर अपराध 24.4% बढ़ गए हैं।

सामान्य साइबर सुरक्षा मिथक

- केवल मज़बूत पासवर्ड ही पर्याप्त सुरक्षा है
- प्रमुख साइबर सुरक्षा जोखिम सर्वविदित हैं
- सभी साइबर हमले वैक्टर (vector) निहित होते हैं
- साइबर अपराधी छोटे व्यवसायों पर हमला नहीं करते हैं

साइबर वॉर

- किसी दूसरे के कंप्यूटर सिस्टम को बाधित करने, क्षति पहुँचाने या नष्ट करने के लिये किये गए डिजिटल हमले।

CYBER THREAT ACTORS

CYBER THREAT ACTOR	MOTIVATION
NATION-STATES	GEOPOLITICAL
CYBERCRIMINALS	PROFIT
HACKTIVISTS	IDEOLOGICAL
TERRORIST GROUPS	IDEOLOGICAL VIOLENCE
THRILL-SEEKERS	SATISFACTION
INSIDER THREATS	DISCONTENT

साइबर सुरक्षा के प्रकार

- महत्त्वपूर्ण बुनियादी ढाँचा सुरक्षा (रोबस्ट एक्सेस कंट्रोल)
- नेटवर्क सुरक्षा (डिप्लॉयिंग फायरवॉल)
- एप्लिकेशन सुरक्षा (कोड रिव्यू)
- क्लाउड सुरक्षा (टोकनाइज़ेशन)
- सूचना सुरक्षा (डेटा मास्किंग)

हाल ही में हुए प्रमुख साइबर हमले

- वान्नाक्राई रैनसमवेयर अटैक (वर्ष 2017)
- कैम्ब्रिज एनालिटिका डेटा ब्रीच (वर्ष 2018)
- 9M+ कार्डधारकों का वित्तीय डेटा लीक, जिसमें SBI भी शामिल है (वर्ष 2022)

विनियम एवं पहलें

- **अंतर्राष्ट्रीय स्तर पर:**
  - साइबर स्पेस में राज्यों के उत्तरदायी व्यवहार को बढ़ावा देने से संबंधित संयुक्त राष्ट्र के सरकारी विशेषज्ञों के समूह (GGE)।
  - नाटो का कोऑपरेटिव साइबर डिफेंस सेंटर ऑफ एक्सीलेंस (CCDCOE)
  - साइबर अपराध पर बुडापेस्ट कन्वेंशन, 2001 (भारत हस्ताक्षरकर्त्ता नहीं है)
- **भारतीय स्तर पर:**
  - IT अधिनियम, 2000 (धारा 43, 66, 66B, 66C, 66D)
  - राष्ट्रीय साइबर सुरक्षा नीति, 2013
  - नेशनल साइबर सिक्योरिटी स्ट्रेटेजी, 2020
  - साइबर सुरक्षित भारत पहल
  - भारतीय साइबर अपराध समन्वय केंद्र (I4C)
  - कंप्यूटर आपातकालीन प्रतिक्रिया टीम - भारत (CERT-In)

साइबर सुरक्षा के लिये उठाए जाने वाले आवश्यक कदम

- नेटवर्क सुरक्षा
- मैलवेयर सुरक्षा
- इंसिडेंट मैनेजमेंट
- उपयोगकर्त्ता को शिक्षित और जागरूक करना
- सुरक्षित विन्यास
- उपयोगकर्त्ता के विशेषाधिकारों का प्रबंधन करना
- सूचना जोखिम प्रबंधन व्यवस्था

Drishti IAS

आगे की राह

- **साइबर सुरक्षा संवर्द्धन: बैंकों और प्रौद्योगिकी सेवा प्रदाताओं को एंडपॉइंट सुरक्षा, नेटवर्क सुरक्षा, डेटा बैकअप तथा कर्मचारी प्रशिक्षण सहित मज़बूत साइबर सुरक्षा उपायों को लागू करना होगा।**
    - खतरे का पता लगाने और रोकथाम के कारण वर्ष 2022 व 2023 के बीच रैनसमवेयर इन्फेक्शन में 11.5% की गिरावट आई है।
    - **बैंकों और वित्तीय संस्थानों के बीच खतरे** की खुफिया जानकारी साझा करने के लिये एक केंद्रीकृत मंच स्थापित करना।
- **डेटा बैकअप और रिकवरी: ऑफलाइन बैकअप सहित मज़बूत डेटा बैकअप और रिकवरी प्रक्रियाओं को लागू करना। साइबर हमले की स्थिति में न्यूनतम व्यवधान सुनिश्चित करने के लिये व्यापक व्यवसाय निरंतरता योजनाएँ विकसित करना।**
- **उन्नत सुरक्षा मानक:** तृतीय-पक्ष विक्रेताओं और भागीदारों का कठोर सुरक्षा मूल्यांकन करना। साइबर हमलों के प्रभाव को कम करने के लिये घटना प्रतिक्रिया क्षमताओं में सुधार करना।
    - सुरक्षा के प्रति प्रतिबद्धता प्रदर्शित करने के लिये प्रासंगिक **साइबर सुरक्षा प्रमाण-पत्र** प्राप्त करना।

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)