LockBit रैनसमवेयर

प्रलिमि्स के लयि:

LockBit रैनसमवेयर, साइबर अटैक, साइबर-क्राइम, क्रप्टिो वायरस, साइबर सुरक्षति भारत, साइबर स्वच्छता केंद्र।

मेन्स के लयि:

LockBit रैनसमवेयर और इसके वरिुद्ध सुरक्षा, भारत में साइबर हमलों के उदाहरण, भारत में साइबर अपराध का बढ़ता खतरा और राष्ट्रीय सुरक्षा पर इसका प्रभाव।

चर्चा में क्यों?

हाल ही में **LockBit रैनसमवेयर** द्वारा Mac उपकरणों को लक्षति करने का मामला सामने आया है।

- इससे पहले जनवरी 2023 में कथति तौर पर ब्रटिेन की डाक सेवाओं पर साइबर हमले के पीछे LockBit गैंग का हाथ था, जसिसे अंतर्राष्ट्रीय शपिगि बाधति हो गई थी।
- रैनसमवेयर एक प्रकार का मैलवेयर है जो कंप्यूटर डेटा को हाईजैक कर लेता है और उस डेटा को वापस बहाल करने के बदले फरिौती (आमतौर पर बटिकॉइन में) की मांग करता है।

LockBit रैनसमवेयर:

- **परचिय**:
  - LockBit, जसि पहले "ABCD" रैनसमवेयर के रूप में जाना जाता था, एक प्रकार का कंप्यूटर वायरस है जो कसिी के कंप्यूटर में प्रवेश कर **महत्त्वपूर्ण फाइलों को एन्क्रप्टि करता** है ताकि उन्हें एक्सेस न कयिा जा सके।
    - यह वायरस पहली बार सतिंबर 2019 में पाया गया था और इसे "**क्रप्टिो वायरस**" कहा जाता है क्योंकि यह पीड़ति की फाइल को डक्रिप्टि करने के लयि क्रप्टिोकरेंसी में भुगतान की मांग करता है।
  - LockBit का उपयोग आमतौर पर उन कंपनयिों या संगठनों पर हमला करने के लयि कयिा जाता है जो अपनी **फाइलों को वापस पाने के लयि बहुत अधकि कीमत देने के लयि तैयार होते हैं।**
  - इस संबंध में डार्क वेब पर एक वेबसाइट है जसिमें उन सदस्यों और पीड़तिों का ववरिण होता है जो भुगतान करने से इनकार करते हैं।
  - LockBit का उपयोग **यू.एस., चीन, भारत, यूक्रेन और यूरोप** सहति कई अलग-अलग देशों में कंपनयिों को लक्षति करने के लयि कयिा गया है।
- **कार्य प्रणाली:**
  - यह अपनी हानकिारक (नुकसान पहुँचाने वाली) **फाइलों को हानरिहति छवि वाली फाइलों** की तरह बनाकर छुपाता है। LockBit भरोसेमंद होने का नाटक कर लोगों को कंपनी के नेटवर्क तक पहुँच प्रदान करने के लयि उन्हें झाँसा देता है।
  - एक बार सस्टिम में प्रवेश करने के बाद **LockBit कंपनी को उसकी फाइलों को पुनर्प्राप्त करने में मदद करने वाली सभी सुवधिाओं को अक्षम कर देता है** और सभी फाइलों को इस प्रकार प्रबंधति करता है कि उन्हें कसिी वशिेष कुंजी के बनिा खोला नही जा सकता जो केवल LockBit गरिोह के पास होती है।
  - इससे प्रभावति व्यक्ति/संस्था के पास LockBit गरिोह से संपर्क करने और डेटा के लयि भुगतान करने के अलावा कोई वकिल्प नहीं बचता है। इस डेटा को ये गरिोह डार्क वेब पर बेच सकते हैं भले ही उन्हें इसका भुगतान कयिा जाए अथवा नहीं।
- **LockBit गैंग:**
  - **LockBit** गैंग/गरिोह साइबर अपराधयिों का एक समूह है जो धन की वसूली के लयि **सर्वसि मॉडल के रूप मे रैनसमवेयर** का उपयोग करता है।
  - वे इस प्रकार के हमले कसिी के आदेश पर करते हैं जसिके लयि उन्हें भुगतान प्राप्त होता है और फरि भुगतान राशि को अपनी टीम और

सहयोगियों में बाँट लेते हैं।

- वे अत्यधिक कुशल होते हैं और पकड़ में आने से बचने के लिये रूसी व्यवस्था अथवा **स्वतंत्र राज्यों के राष्ट्रमंडल (Commonwealth of Independent States)** पर हमला नहीं करते हैं।

LockBit द्वारा mac OS को लक्षित करने का कारण:

- **LockBit** अपने हमलों के दायरे का विस्तार करने और संभावित रूप से **अपने वित्तीय लाभ को बढ़ाने के तरीके के रूप में mac OS को लक्षित कर रहा है।**
  - हालाँकि ऐतिहासिक रूप से **रैनसमवेयर ने मुख्य रूप से विंडोज़, लाइनक्स और वीएमवेयर ESXi सर्वरों को लक्षित किया है,** यह अब mac OS के लिये एन्क्रिप्टर्स का परीक्षण कर रहा है।
- ऐसा पाया गया है कि वर्तमान एन्क्रिप्टर्स पूरी तरह से चालू नहीं हो पाए हैं लेकिन इस बात से भी इनकार नहीं किया जा सकता कि ये **समूह mac OS को लक्षित करने के लिये सक्रिय रूप से एक पृथक उपकरण/तकनीक विकसित कर रहे हैं।**
- इन सभी का उद्देश्य विभिन्न प्रणालियों/सिस्टम्स को लक्षित करके रैनसमवेयर ऑपरेशन की सहायता से अधिक पैसा वसूलना है।

भारत में साइबर हमले की हालिया घटनाएँ:

- वर्ष 2020 में लगभग 82% कंपनियों के प्रभावित होने के साथ भारत में रैनसमवेयर हमलों में उल्लेखनीय वृद्धि देखने को मिली है।
- हाल के वर्षों में कई हाई-प्रोफाइल हमले हुए हैं, जिनमें वर्ष 2017 का **वानाक्राई हमला, Juspay के डेटा उल्लंघन का मामला** शामिल है। इसने वर्ष 2021 में अमेज़न सहित 35 मिलियन ग्राहकों को प्रभावित किया और हाल ही में दिसंबर 2022 में [दिल्ली स्थित एम्स भी रैनसमवेयर हमले का शिकार हुआ।]
  - **वर्ष 2022 में एयर इंडिया को एक बड़े साइबर हमले का सामना करना पड़ा**, जिसमें पासपोर्ट, टिकट और क्रेडिट कार्ड की जानकारी सहित 4.5 मिलियन ग्राहक रिकॉर्ड से समझौता किया गया।

साइबर सुरक्षा से संबंधित वर्तमान सरकार की पहल:

- भारतीय साइबर अपराध समन्वय केंद्र (I4C)
- भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (CERT-In)
- साइबर सुरक्षित भारत पहल
- साइबर स्वच्छता केंद्र
- राष्ट्रीय साइबर सुरक्षा समन्वय केंद्र (NCCC)
- साइबर बीमा नीति
- केरल सरकार साइबरडोम परियोजना

LockBit रैनसमवेयर से बचाव:

- **मज़बूत पासवर्ड:**
  - खाता सुरक्षा का उल्लंघन प्रायः कमज़ोर पासवर्ड के कारण होता है क्योंकि हैकर्स इसे आसानी से अनुमान लगा सकता है या एल्गोरिद्म टूल को क्रैक कर सकता है। अतः सुरक्षा के लिये **मज़बूत पासवर्ड चुनें जो लंबा होने के साथ ही उसमें अलग-अलग तरह के कैरेक्टर हों।**
- **बहु-कारक प्रमाणीकरण:**
  - ब्रूट फोर्स अटैक को रोकने हेतु अपने **सिस्टम में लॉग इन करते समय अपने पासवर्ड के अलावा बायोमेट्रिक्स (जैसे- फिंगरप्रिंट या चेहरे की पहचान) या वास्तविक USB कुंजी** प्रमाणक का उपयोग करना चाहिये।
    - ब्रूट फोर्स अटैक एक प्रकार का साइबर हमला है जहाँ **हमलावर वर्णों के विभिन्न संयोजनों को बार-बार आज़माकर एक पासवर्ड का अनुमान लगाने** की कोशिश करते हैं जब तक कि उन्हें सही पासवर्ड नहीं मिल जाता।
- **खाता अनुमति का पुनर्मूल्यांकन:**
  - सुरक्षा जोखिमों को कम करने हेतु उपयोगकर्त्ता अनुमति पर कड़े प्रतिबंध लगाना महत्त्वपूर्ण है। यह विशेष रूप से दूसरे छोर पर (Endpoint) उपयोगकर्त्ताओं द्वारा उपयोग किये जाने वाले संसाधनों एवं प्रशासनिक पहुँच वाले IT खातों के लिये महत्त्वपूर्ण है।
  - साथ ही यह भी सुनिश्चित करना आवश्यक है कि **वेब डोमेन, सहयोगी प्लेटफॉर्म, वेब मीटिंग सेवाएँ और एंटरप्राइज़ डेटाबेस** सभी सुरक्षित हों।
- **तंत्र-व्यापी बैकअप:**

- स्थायी डेटा हानि से बचने हेतु अपने **महत्त्वपूर्ण डेटा का ऑफलाइन बैकअप बनाना महत्त्वपूर्ण है।**
- यह सुनिश्चित करने हेतु समय-समय पर बैकअप बनाकर अपने सिस्टम की अप-टू-डेट कॉपी सुनिश्चित करना। किसी मैलवेयर से संक्रमित होने की स्थिति में एक स्वच्छ बैकअप चुनने में सक्षम होने हेतु कई बैकअप साइट्स तथा उन्हें बदलने का विकल्प खुला रखना चाहिये।

UPSC सिविल सेवा परीक्षा, विगत वर्ष के प्रश्न (PYQ):

??????????:

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 किसी व्यक्ति के साइबर बीमा कराने पर निधि की हानि की भरपाई एवं अन्य लाभों के अतिरिक्त सामान्यतः निम्नलिखित में से कौन-कौन से लाभ दिये जाते हैं?(2020)

1. यदि कोई मैलवेयर कंप्यूटर तक उसकी पहुँच बाधित कर देता है, तो कंप्यूटर प्रणाली को पुन प्रचालित करने में लगने वाली लागत।
2. यदि यह प्रमाणित हो जाता है कि किसी शरारती तत्त्व द्वारा जान-बूझकर कंप्यूटर को नुकसान पहुँचाया गया है तो नए कंप्यूटर की लागत।
3. यदि साइबर बलात-ग्रहण होता है तो इस हानि को न्यूनतम करने के लिये विशेषज्ञ परामर्शदाता की सेवाएँ लेने पर लगने वाली लागत।
4. यदि कोई तीसरा पक्ष मुकदमा दायर करता है तो अदालत में बचाव करने में लगने वाली लागत।

नीचे दिये गए कूट का प्रयोग कर सही उत्तर चुनिये:

(a) केवल 1, 2 और 4
(b) केवल 1, 3 और 4
(c) केवल 2 और 3
(d) 1, 2, 3 और 4

उत्तर: (b)

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. भारत की आंतरिक सुरक्षा को ध्यान में रखते हुए सीमा पार से होने वाले साइबर हमलों के प्रभाव का विश्लेषण कीजिये। साथ ही इन परिष्कृत हमलों के विरुद्ध रक्षात्मक उपायों की चर्चा कीजिये। **(2021)**

प्रश्न. विभिन्न प्रकार के साइबर अपराधों और खतरे से लड़ने के लिये आवश्यक उपायों पर चर्चा कीजिये। **(2020)**

स्रोत: द हिंदू