अकीरा रैनसमवेयर

हाल ही में भारत सरकार की कंप्यूटर इमरजेंसी रिस्पांस टीम (CERT-In) ने अकीरा रैनसमवेयर के बारे में चेतावनी जारी की है, जो **विंडोज़** और **लिनक्स** दोनों **डिवाइसों** को लक्षित करता है, एक महत्त्वपूर्ण साइबर सुरक्षा **खतरे** के रूप में उभरा है।

- रैनसमवेयर एक प्रकार का **मैलवेयर** है जो **कंप्यूटर डेटा को हाईजैक कर लेता है** और उसे रिकवर करने के लिये **भुगतान (सामान्यतः बिटकॉइन में) की मांग करता है**।

अकीरा रैनसमवेयर:

- **परिचय:**
  - यह **मैलिसियस सॉफ्टवेयर** है जो **डेटा सुरक्षा** के लिये एक महत्त्वपूर्ण खतरा है।
  - यह **विंडोज़ और लिनक्स दोनों डिवाइसों** को लक्षित करने के साथ ही डेटा को हैक करता है और उसे **रिकवर करने के लिये भुगतान** की मांग करता है।
- **अकीरा रैनसमवेयर की मुख्य विशेषताएँ:**
  - इसे **डेटा को एन्क्रिप्ट करने** और एन्क्रिप्टेड फाइल नामों के साथ **"akira" जोड़कर रैनसमवेयर संदेश प्रदान करने** के लिये डिज़ाइन किया गया है।
  - यह एन्क्रिप्शन के दौरान आने वाले व्यवधान को रोकने के लिये **विंडोज शैडो वॉल्यूम** की प्रतियों को हटाने और विंडोज सेवाओं को बंद करने में सक्षम है।
  - यह डिवाइसों को प्रभावित करने के लिये **VPN सेवाओं और मैलिसियस फाइलों** के माध्यम से हैकिंग करता है, जिससे इसका पता लगाना और रोकना चुनौतीपूर्ण हो जाता है।
- **संचालन का तरीका:**
  - अकीरा रैनसमवेयर विभिन्न रूपों में फैलता है, जिसमें **मैलिसियस अटैचमेंट** के साथ स्पीयर फिशिंग ई-मेल, **ड्राइव-बाय डाउनलोड और विशेष रूप से तैयार किये गए वेब लिंक** शामिल हैं।
  - **असुरक्षित रिमोट डेस्कटॉप कनेक्शन** रैनसमवेयर ट्रांसमिशन का एक और रूप है।
- **अकीरा हमले के निहितार्थ:**
  - अकीरा रैनसमवेयर से एक बार प्रभावित होने से **संवेदनशील डेटा चोरी हो जाता है, यह डेटा को एन्क्रिप्ट कर देता है, जिससे डेटा वापस पीड़ित के पास नहीं पहुँच पाता है।**
  - फिर हमलावर डिक्रिप्शन के लिये फिरौती की मांग करते हैं और उनकी मांग पूरी नहीं होने पर चुराए गए डेटा को **डार्क वेब** पर लीक करने की धमकी देते हैं।
- **अकीरा रैनसमवेयर के विरुद्ध सुरक्षा उपाय:**
  - किसी भी हमले की **स्थिति में डेटा हानि को रोकने के लिये नियमित रूप से नवीनतम ऑफलाइन बैकअप** बनाए रखना।
  - संभावित भेद्यता को दूर करने हेतु पुराने सिस्टम के लिये वर्चुअल चिप्पी (Patching) सहित **ऑपरेटिंग सिस्टम और नेटवर्क को अपडेट** रखें।
  - ई-मेल सत्यापन के लिये **डोमेन-आधारित संदेश प्रमाणीकरण, रिपोर्टिंग और अनुरूपता (Domain-based Message Authentication, Reporting, and Conformance- DMARC), डोमेन की आइडेंटिफाइड मेल (DKIM) और प्रेषक नीति जैसे सुरक्षा प्रोटोकॉल** लागू करना।
  - उपयोगकर्त्ताओं के द्वारा प्रमाणीकरण को बढ़ाने के लिये मज़बूत पासवर्ड नीतियाँ और मल्टी-फैक्टर प्रमाणीकरण (MFA) लागू करना।
  - **बाहरी डिवाइस के उपयोग** के लिये एक कठिन नीति स्थापित करना और **डेटा-एट-रेस्ट तथा डेटा-इन-ट्रांजिट एन्क्रिप्शन सुनिश्चित** करना।
  - दुर्भावनापूर्ण कोड डाउनलोड करने से बचने के लिये .exe, .pif, और .url जैसे संदिग्ध एक्सटेंशन के साथ अटैचमेंट फाइल प्रकारों को ब्लॉक करना।
  - मैलवेयर डाउनलोड को रोकने के लिये उपयोगकर्त्ताओं को संदिग्ध लिंक पर क्लिक करने से सावधान रहने के लिए शिक्षित करें।
  - भेद्यता की पहचान करने और उनका समाधान करने के लिये विशेष रूप से डेटाबेस सर्वर जैसी महत्त्वपूर्ण प्रणालियों हेतु नियमित सुरक्षा ऑडिट करना।

कंप्यूटर इमरजेंसी रिस्पांस टीम-इंडिया (CERT-IN) :

- कंप्यूटर इमरजेंसी रिस्पांस टीम-इंडिया, भारतीय साइबर स्पेस को सुरक्षित करने के उद्देश्य से इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय का संगठन है।
- यह एक **नोडल एजेंसी है जिसका कार्य हैकिंग और फिशिंग जैसे साइबर सुरक्षा** खतरों से निपटना है।
- यह संगठन साइबर **घटनाओं** पर जानकारियों को एकत्र करके, उनका **विश्लेषण और प्रसार करता** है, साथ ही साइबर सुरक्षा घटनाओं पर अलर्ट भी जारी करता है।
- **CERT-IN घटना निवारण और प्रतिक्रिया सेवाओं** के साथ-साथ सुरक्षा गुणवत्ता प्रबंधन सेवाएँ भी प्रदान करता है।

UPSC सिविल सेवा परीक्षा विगत वर्ष के प्रश्न

??????????

प्रश्न. 'वान्नाक्राई, पेट्या और इंटरनलब्लू' पद जो हाल ही में समाचारों में उल्लिखित थे, निम्नलिखित में से किसके साथ संबंधित हैं? (2018)

(a) एक्सोप्लैनेट्स
(b) प्रच्छन्न मुद्रा (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 मालवेयर कंप्यूटर तक उसकी पहुँच बाधित कर देता है, तो कंप्यूटर प्रणाली को पुनः 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 बलात्-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 न्यायालय 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/हैं? (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)

स्रोत: द हिंदू

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/akira-ransomware