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 **वडिोज़** और **लनिक्स** दोनों **डवािइसों** को लक्षति 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 रकिवर करने के लयि **भुगतान (सामान्यतः बटिकॉइन में) की मांग करता है**।

अकीरा रैनसमवेयर:

- **परचिय:**
  - यह **मैलसियिस सॉफ्टवेयर** है जो **डेटा सुरक्षा** के लयि एक महत्त्वपूर्ण खतरा है।
  - यह **वडिोज़ और लनिक्स दोनों डवािइसों** को लक्षति करने के साथ ही डेटा को हैक करता है और उसे **रकिवर करने के लयि भुगतान** की मांग करता है।
- **अकीरा रैनसमवेयर की मुख्य वशिषताएँ:**
  - इसे **डेटा को एन्क्रप्टि करने** और एन्क्रप्टिेड फाइल नामों के साथ **"akira" जोड़कर रैनसमवेयर संदेश प्रदान करने** के लयि डज़िाइन कयिा गया है।
  - यह एन्क्रप्शिन के दौरान आने वाले व्यवधान को रोकने के लयि **वडिोज शैडो वॉल्यूम** की प्रतयिों को हटाने और वडिोज सेवाओं को बंद करने में सक्षम है।
  - यह डवािइसों को प्रभावति करने के लयि **VPN सेवाओं और मैलसियिस फाइलों** के माध्यम से हैकगि करता है, जसिसे इसका पता लगाना और रोकना चुनौतीपूर्ण हो जाता है।
- **संचालन का तरीका:**
  - अकीरा रैनसमवेयर वभिन्नि रूपों में फैलता है, जसिमें **मैलसियिस अटैचमेंट** के साथ स्पीयर फशिगि ई-मेल, **ड्राइव-बाय डाउनलोड और वशिष रूप से तैयार कयि गए वेब लकि** शामलि हैं।
  - **असुरक्षति रमिोट डेस्कटॉप कनेक्शन** रैनसमवेयर ट्रांसमशिन का एक और रूप है।
- **अकीरा हमले के नहितिार्थ:**
  - अकीरा रैनसमवेयर से एक बार प्रभावति होने से **संवेदनशील डेटा चोरी हो जाता है, यह डेटा को एन्क्रप्टि कर देता है, जसिसे डेटा वापस पीड़ति के पास नहीं पहुँच पाता है।**
  - फरि हमलावर डक्रिप्शिन के लयि फरिौती 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 वरिुद्ध सुरक्षा उपाय:**
  - कसिी भी हमले की **स्थतिि में डेटा हानि को रोकने के लयि नयिमति रूप से नवीनतम ऑफलाइन बैकअप** बनाए रखना।
  - संभावति भेद्यता को दूर करने हेतु पुराने सस्टिम के लयि वर्चुअल चप्पिी (Patching) सहति **ऑपरेटगि सस्टिम और नेटवर्क को अपडेट** रखें।
  - ई-मेल सत्यापन के लयि **डोमेन-आधारति संदेश प्रमाणीकरण, रपिोर्टगि और अनुरूपता (Domain-based Message Authentication, Reporting, and Conformance- DMARC), डोमेन की आइडेंटफिाइड मेल (DKIM) और प्रेषक नीति जैसे सुरक्षा प्रोटोकॉल** लागू करना।
  - उपयोगकर्त्ताओं के द्वारा प्रमाणीकरण को बढ़ाने के लयि मज़बूत पासवर्ड नीतयिाँ और मल्टी-फैक्टर प्रमाणीकरण (MFA) लागू करना।
  - **बाहरी डवािइस के उपयोग** के लयि एक कठनि नीति स्थापति करना और **डेटा-एट-रेस्ट तथा डेटा-इन-ट्रांजटि एन्क्रप्शिन सुनश्चिति** करना।
  - दुर्भावनापूर्ण कोड डाउनलोड करने से बचने के लयि .exe, .pif, और .url जैसे संदग्धि एक्सटेंशन के साथ अटैचमेंट फाइल प्रकारों को ब्लॉक करना।
  - मैलवेयर डाउनलोड को रोकने के लयि उपयोगकर्त्ताओं को संदग्धि लकि पर क्लकि करने से सावधान रहने के लए शक्षिति करें।
  - भेद्यता की पहचान करने और उनका समाधान करने के लयि वशिष रूप से डेटाबेस सर्वर जैसी महत्त्वपूर्ण प्रणालयिों हेतु नयिमति सुरक्षा ऑडटि करना।

कंप्यूटर इमरजेंसी रस्पिांस टीम-इंडयिा (CERT-IN) :

- कंप्यूटर इमरजेंसी रस्पिांस टीम-इंडया, भारतीय साइबर स्पेस को सुरक्षति करने के उद्देश्य से इलेक्ट्रॉनक्सि और सूचना प्रौद्योगकिी मंत्रालय का संगठन है।
- यह एक **नोडल एजेंसी है जसिका कार्य हैकगि और फशिगि जैसे साइबर सुरक्षा** खतरों से नपिटना है।
- यह संगठन साइबर **घटनाओं** पर जानकारयिों को एकत्र करके, उनका **वशि्लेषण और प्रसार करता** है, साथ ही साइबर सुरक्षा घटनाओं पर अलर्ट भी जारी करता है।
- **CERT-IN घटना नविारण और प्रतक्रियिा सेवाओं** के साथ-साथ सुरक्षा गुणवत्ता प्रबंधन सेवाएँ भी प्रदान करता है।

UPSC सविलि सेवा परीक्षा वगित वर्ष के प्रश्न

??????????

प्रश्न. 'वान्नाक्राई, पेट्या और इंटर्नलब्लू' पद जो हाल ही में समाचारों में उल्लखिति थे, नम्निलखिति में से कसिके साथ संबंधति हैं? (2018)

(a) एक्सोप्लैनेट्स
(b) प्रच्छन्न मुद्रा (क्रप्टिोकरेंसी)
(c) साइबर आक्रमण
(d) लघु उपग्रह

उत्तर: (c)

प्रश्न. भारत में, कसिी व्यक्ति के साइबर बीमा कराने पर नधि की हानि की भरपाई एवं अन्य लाभों के अतरिक्ति सामान्यत: नम्निलखिति में से कौन-कौन से लाभ दयि जाते हैं? (2020)

1. यदि कोई मालवेयर कंप्यूटर तक उसकी पहुँच बाधति कर देता है, तो कंप्यूटर प्रणाली को पुन: प्रचालति करने में लगने वाली लागत
2. यदि यह प्रमाणति 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 लयि वशिषज्ञ 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 दयि गए कूट का प्रयोग कर सही उत्तर चुनयि-

(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 रपिोर्ट करना नम्निलखिति में से कसिके/कनिके लयि वधितिः अधदिशात्मक है/हैं? (2017)

1- सेवा प्रदाता (सर्वसि प्रोवाइडर)
2- डेटा सेंटर
3- कॉर्पोरेट नकिाय बॉडी (कॉर्पोरेट)

नीचे दयि गए कूट का प्रयोग कर सही उत्तर चुनयि:

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

उत्तर: (d)

स्रोत: द हदि्