पेगासस स्पायवेयर

प्रिलिम्स के लिये:

[पेगासस स्पायवेयर](), ज़ीरो-क्लिक तथा ज़ीरो-डे वल्नरेबिलिटीज़, [राष्ट्रीय साइबर सुरक्षा रणनीति](), [साइबर सुरक्षित भारत]()

मेन्स के लिये:

स्पायवेयर तथा निजता संबंधी चिंताएँ, साइबर हमले, सरकारी पहल

[स्रोत: द हिंदू]()

चर्चा में क्यों?

[पेगासस स्पायवेयर]() के कारण पुनः एक बार निजता और सुरक्षा संबंधी मुद्दे चर्चा में आए हैं। **एमनेस्टी इंटरनेशनल** की हालिया रिपोर्टें **दो प्रमुख भारतीय पत्रकारों के फोन** को लक्षित करने में इसके उपयोग की ओर संकेत करती हैं, जिससे संभावित सरकारी भागीदारी के बारे में पूछताछ शुरू हो गई है।

- एमनेस्टी इंटरनेशनल 10 मिलियन से अधिक लोगों का एक वैश्विक आंदोलन है जो एक ऐसे भविष्य की परिकल्पना के लिये प्रतिबद्ध है जहाँ **सभी के मानवाधिकारों को सुनिश्चित** किया जा सके।

पेगासस स्पायवेयर क्या है?

- **परिचय:**
  - पेगासस स्पायवेयर एक **अत्यधिक सुदृढ़ मोबाइल आवेक्षण टूल** है जो विभिन्न ऐप्स और स्रोतों से डेटा तथा जानकारी एकत्र कर सेलफोन तक गुप्त रूप से पहुँच सकता है एवं निगरानी कर सकता है।
  - इसे **इज़रायली साइबर-इंटेलिजेंस फर्म NSO ग्रुप** द्वारा विकसित किया गया था, जो इसे मात्र अपराध तथा आतंकवाद की रोकथाम के लिये सरकारी एजेंसियों को बेचने का दावा करता है।
    - NSO उन पत्रकारों, वकीलों तथा मानवाधिकार रक्षकों को निशाना बनाने से बचने के लिये सुरक्षा उपायों पर ज़ोर देता है जो आतंक अथवा गंभीर अपराधों में शामिल नहीं हैं।
- **परिचालन प्रक्रिया:**
  - पेगासस डिवाइस को लक्षित करने के लिये **"ज़ीरो-क्लिक"** विधियों का उपयोग करता है, यह एक सॉफ्टवेयर है जो **उपयोगकर्त्ता की सहमति के बिना उसके डिवाइस पर स्पायवेयर इंस्टॉल करने की अनुमति** देता है।
    - स्पायवेयर को **इंस्टॉलेशन के लिये** किसी **उपयोगकर्त्ता कार्रवाई** की आवश्यकता नहीं होती है जो इसे **नियमित ऐप्स** से अलग करता है जिनके **इंस्टॉलेशन में स्पष्ट उपयोगकर्त्ता पुष्टि की आवश्यकता होती है।**
    - यह व्हाट्सएप, आईमैसेज या फेसटाइम जैसे ऐप्स में कमज़ोरियों का फायदा उठा सकता है और एक संदेश या कॉल भेज सकता है जो स्पायवेयर की स्थापना को ट्रिगर करता है, भले ही उपयोगकर्त्ता इसे न देखें या इसका जवाब न दें।
  - पेगासस एक स्पायवेयर है जो एप्पल उत्पादों पर स्पायवेयर तैनात करने के लिये **ज़ीरो-डे भेद्यता की कमज़ोरियों** का लाभ उठा सकता है।
    - ज़ीरो-डे भेद्यता एक ऑपरेटिंग सिस्टम में एक **अनदेखा दोष या बग** है जिसके बारे में मोबाइल फोन के निर्माता को अभी तक पता नहीं लग पाया है और इसलिये वह **इसे ठीक करने में सक्षम नहीं** है।
- **लक्ष्य:**
  - कई जाँचों और रिपोर्टों से पता चला है कि पेगासस स्पायवेयर का इस्तेमाल **पत्रकारों, मानवाधिकार कार्यकर्त्ताओं, वकीलों, विपक्षी नेताओं** और **राष्ट्राध्यक्षों की जासूसी करने के लिये** किया गया है।
  - जिन देशों पर अपने आलोचकों और दुश्मनों को निशाना बनाने के लिये पेगासस स्पायवेयर का उपयोग करने का आरोप लगाया गया है उनमें **सऊदी अरब, मैक्सिको, भारत, मोरक्को, हंगरी, अज़रबैजान** तथा **रवांडा** शामिल हैं।
- **आशय:**
  - पेगासस स्पायवेयर भ्रष्टाचार को उजागर करने, मानवाधिकारों की रक्षा करने तथा लोकतंत्र का समर्थन करने वाले **व्यक्तियों एवं समूहों की [गोपनीयता और सुरक्षा]()** को खतरे में डालता है।

    - यह पत्रकारों के स्रोतों, तरीकों और सामग्रियों को उजागर करके, उनकी स्वतंत्रता से समझौता करके प्रेस की स्वतंत्रता को कमज़ोर करता है।
    - स्पायवेयर राष्ट्रों की संप्रभुता और स्थरिता के लयि खतरा उत्पन्न करता है, **आंतरकि मामलों एवं नरि्णय लेने की प्रक्रयिाओं में वदिशी हस्तक्षेप तथा जासूसी को सक्षम बनाता** है।
- **चुनौतियाँ:**
    - पेगासस स्पायवेयर का पता लगाना और उसे हटाना मुश्कलि है, क्योंकि यह डिवाइस पर अपनी उपस्थिति एवं गतविधि को छिपा सकता है तथा अगर इसे पता चलता है कि इसकी खोज या वश्लिेषण कयिा जा रहा है तो यह **स्वयं को नष्ट कर सकता** है।
    - कानूनी रूप से अस्पष्ट क्षेत्रों में इसके संचालन के कारण पेगासस स्पायवेयर को वनियिमति और नयिंत्रति करना मुश्कलि है।
        - NSO समूह और उसके ग्राहक आमतौर पर स्पायवेयर के दुरुपयोग के लयि ज़म्मिदारी से इनकार करते हैं या उससे बचते हैं।

साइबर खतरों के प्रमुख प्रकार:

Cyber Threat	Description
Malware	Malicious software designed to harm or exploit systems by infecting, disrupting, or gaining unauthorized access.
Phishing	Deceptive attempts to acquire sensitive information, often through fake emails, websites, or messages impersonating trusted entities.
Ransomware	Encrypts data and demands payment (usually in cryptocurrency) for its release, posing significant threats to data integrity.
DDoS Attacks	Overwhelms a system with a flood of traffic, causing service disruption by exhausting resources or bandwidth.
Man-in-the-Middle (MitM)	Intercepts and potentially alters communication between two parties, leading to unauthorized access or information theft.
SQL Injection	Exploits vulnerabilities in SQL databases by injecting malicious code, allowing unauthorized access or data manipulation.
Zero-Day Exploits	Attacks targeting undiscovered vulnerabilities in software before developers can create a patch, posing a serious and often potent threat.
Social Engineering	Manipulating individuals into divulging sensitive information through psychological manipulation or deception.
Insider Threats	Risks originating from individuals within an organization, either intentionally or unintentionally causing harm or data breaches.
Advanced Persistent Threats (APTs)	Prolonged and targeted cyber attacks often linked to espionage, aiming to infiltrate and remain undetected in a network.
Cross-Site Scripting (XSS)	Injects malicious scripts into web pages viewed by others, potentially compromising the security and privacy of users.
Credential Stuffing	Uses stolen usernames and passwords from one breach to gain unauthorized access to other accounts due to individuals reusing passwords.
Internet of Things (IoT) Threats	Exploits vulnerabilities in connected devices, potentially allowing unauthorized access or disruption of IoT networks.
Cryptojacking	Unauthorized use of a computer's resources for cryptocurrency mining, slowing down systems and consuming energy without the user's consent.
Wi-Fi Eavesdropping	Unauthorized interception of wireless communication, where attackers may capture sensitive data transmitted over Wi-Fi networks.

The Vision

संबंधित साइबर सुरक्षा पहल क्या हैं?

- **भारत:**
  - सूचना प्रौद्योगिकी अधिनियम, 2000
  - राष्ट्रीय साइबर सुरक्षा रणनीति
  - साइबर सुरक्षित भारत
  - कंप्यूटर आपातकालीन प्रतिक्रिया टीम - भारत (CERT-In)
  - महत्त्वपूर्ण सूचना अवसंरचना
  - भारतीय साइबर अपराध समन्वय केंद्र (I4C)
- **अंतर्राष्ट्रीय तंत्र:**
  - **अंतर्राष्ट्रीय दूरसंचार संघ (ITU)**
  - **साइबर अपराध पर बुडापेस्ट कन्वेंशन**

आगे की राह

- निगरानी उपकरणों के किसी भी अनैतिक उपयोग के लिये कंपनियों को जवाबदेह ठहराने और स्वतंत्र ऑडिट की सुविधा के लिये एक **अंतर्राष्ट्रीय निरीक्षण तंत्र** स्थापित की जानी चाहिये।
  - **स्पायवेयर के उपयोग को स्पष्ट रूप से प्रतिबंधित करने** और लक्षित व्यक्तियों की गोपनीयता एवं मानवाधिकारों की रक्षा के लिये राष्ट्रीय व अंतर्राष्ट्रीय कानूनी ढाँचे को मज़बूत की जानी चाहिये।
- स्पायवेयर से उत्पन्न जोखिमों और संभावित घुसपैठ के खिलाफ अपने उपकरणों की सुरक्षा के बारे में **लोगों को शिक्षित करने के लिये जन जागरूकता अभियान चलाएँ।**
- संभावित स्पायवेयर गतिविधियों की निरंतर निगरानी सहित साइबर खतरों का सक्रिय रूप से पता लगाने और उन्हें बेअसर करने के लिये **राष्ट्रीय साइबर सुरक्षा बुनियादी ढाँचे को मज़बूत** करें।
- तकनीकी कंपनियों को **नैतिक दिशा-निर्देशों को अपनाने के लिये प्रोत्साहित करें** जो मानवाधिकार सिद्धांतों के अनुरूप हों तथा ज़िम्मेदार कॉर्पोरेट व्यवहार को बढ़ावा दें।

UPSC सिविल सेवा परीक्षा, विगत वर्ष प्रश्न

[illegible]:

प्रश्न1. 'वान्नाक्राई, पेट्या और इंटर्नलब्लू' 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)

प्रश्न2. भारत में, किसी व्यक्ति के साइबर बीमा कराने पर निधि की हानि की भरपाई एवं अन्य लाभों के अतिरिक्त सामान्यत: 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 पुन: प्रचालित करने में लगने वाली लागत।
2. यदि यह प्रामाणित 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)

प्रश्न1. 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 नकािय 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)

?????:

प्रश्न1. साइबर सुरक्षा के वभिन्नि तत्त्व क्या हैं? साइबर सुरक्षा में चुनौतयिों को ध्यान में रखते हुए समीक्षा कीजयि कि भारत ने कसि हद तक एक व्यापक राष्ट्रीय साइबर सुरक्षा रणनीति सफलतापूर्वक वकिसति की है। (2022)

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/pegasus-spyware-2