

पेगासस सपायवेयर

प्रलिस के लयल:

पेगासस सपायवेयर, ज़ीरो-कलकल तथा ज़ीरो-डे वलनरेबलललललल, [राषलरीय साइबर सुरकषा रणनीतल](#), [साइबर सुरकषतल भारत](#)

मेन्स के लयल:

सपायवेयर तथा नजलतल संबंघी कलतलएँ, साइबर हमले, सरकारी पहल

[सुरत: द हदु](#)

कलरुा में कलरुु?

[पेगासस सपायवेयर](#) के कारण पुन: एक बार नजलतल और सुरकषा संबंघी मुदुदे कलरुा में आए हैं। [एमनेसुटी इंटरनेशनल](#) की हालयल रलरुुलरुु [दु प्रमुख भारतीय पलरुुकलरुु के फुन](#) कु लकषतल करने में इसके उलयुग की ओर संकुक कलरुुती हैं, जसलसे संभलवतल सरकारी भलगीदारी के बारे में पूछतलछ शुरु हु गई है।

- एमनेसुटी इंटरनेशनल 10 मलयलन से अधकल लुगुु कल एक वैशुवलकल आंदुलन है कु एक ऐसे भुवषुय की पलरुकलरुुपनल के लयल पलरुुतलबलदुध है जहसुुभी के मलनवलधकलरुु कल सुनशुुकलतल कयल जल सके।

पेगासस सपायवेयर कलरुु है?

पलरुुकलरुु:

- पेगासस सपायवेयर एक अतुयधकल सुदुदुदु मलबलइल आवुकषण दुल है कु वलभलनलन ऐप्स और सुरतुुतुु से डुकल तथा जलनकलरी एकतुर कल सेलफुन तक गुपुत रुु से पहुँक सकतल है एवं नगलरलनी कल सकतल है।
- इसे [इज़रलयली साइबर-इंटेल्जलंस फलरुु NSO गुपु](#) दुवलरल वकलसतल कयल गयल थल, कु इसे मलतुर अपलरलध तथा आतंकवलद की रुकथलम के लयल सरकारी एजेंसलरुु कल बेकने कल दुवल कलरुुतल है।
 - NSO उन पलरुुकलरुु, वकीलुु तथा मलनवलधकलरुु रकषकुु कल नशलनल बनलने से बकने के लयल सुरकषल उलयुु पलरुु जुर देतल है कु आतंक अथवल गंभीर अपलरलधुु में शलमलल नही है।

पलरुुकलरुुलन पलरुुकलरुु:

- पेगासस डवलइस कु लकषतल करने के लयल “[ज़ीरो-कलकल](#)” वधलरुु कल उलयुग कलरुुतल है, यल एक सॉफुतुवेयर है कु उलयुगकलरुुतल की सहमतल के बनल उसके डवलइस पलरुु सपायवेयर इंसुतुल कलरुुतल की अनुमतल देतल है।
 - सपायवेयर कु इंसुतुललेशन के लयल कलसी उलयुगकलरुुतल कलरुुवरलई की आवशुयकतल नही हुती है कु इसे नयलमतल ऐप्स से अलग कलरुुतल है जलनके इंसुतुललेशन में स्पषुत उलयुगकलरुुतल पुषुतल की आवशुयकतल हुती है।
 - यल वलहलटसएप, आईमेसेज यल फेसुतलइम जैसे ऐप्स में कलमजुरलरुु कल फलयदल उठल सकतल है और एक संदुश यल कुल भेज सकतल है कु सपायवेयर की सुथलपनल कु दुरगलर कलरुुतल है, भले ही उलयुगकलरुुतल इसे न देखें यल इसकल जवलब न दें।
- पेगासस एक सपायवेयर है कु एप्पल उतुपलदुु पलरुु सपायवेयर तैनलत करने के लयल [ज़ीरो-डे भेदुयतल की कलमजुरलरुु कल](#) ललभ उठल सकतल है।
 - ज़ीरो-डे भेदुयतल एक ऑपलरुुतगल सलसुतलम में एक अनदुखल दुष यल बग है जसलके बारे में मलबलइल फुन के नलरुुमलतल कु अभी तक पतल नही लग पलयल है और इसललयल वल इसे ठीक कलरुुतल में सकषम नही है।

लकषुय:

- कुई जलँकुु और रलरुुलरुु से पतल कलरुु है कल पेगलसस सपायवेयर कल इसुतेमलपलरुुकलरुु, मलनवलधकलरुु कलरुुकलरुुतलओु, वकीलुु, वपलकषी नेतलओु और [राषुतरलधुयकषु कल जलसुुसी करने के लयल](#) कयल गयल है।
- जलन देशुु पलरुु अपने आलुककुु और दुशुमनुु कल नशलनल बनलने के लयल पेगलसस सपायवेयर कल उलयुग करने कल आरुुप लगलयल गयल है उनमें [सकुदुी अरब, मैक्सकुु, भारत, मलरककुु, हंगरी, अज़रबैजलन](#) तथा [रवलंडल](#) शलमलल हैं।

आशुय:

- पेगलसस सपायवेयर भुरषुतलकलरुु कु उजलग कलरुुतल, मलनवलधकलरुु कल रकषल करने तथा लुकतंतुर कल सलमरुुथन करने वललेधुयकलरुुतलरुु एवं सलमूहुु कल [गुुपनीयतल और सुरकषल](#) कु खतरे में डललतल है।

- यह पत्रकारों के स्रोतों, तरीकों और सामग्रियों को उजागर करके, उनकी स्वतंत्रता से समझौता करके प्रेस की स्वतंत्रता को कमजोर करता है।
- स्पायवेयर राष्ट्रों की संप्रभुता और स्थिरता के लिये खतरा उत्पन्न करता है, **आंतरिक मामलों एवं नरिणय लेने की प्रक्रियाओं में वदेशी हस्तक्षेप तथा जासूसी को सक्षम बनाता है।**

▪ **चुनौतियाँ:**

- पेगासस स्पायवेयर का पता लगाना और उसे हटाना मुश्किल है, क्योंकि यह डेविड्स पर अपनी उपस्थिति एवं गतिविधियों को छिपा सकता है तथा अगर इसे पता चलता है कइसकी खोज या विश्लेषण किया जा रहा है तो यह **स्वयं को नष्ट कर सकता है।**
- कानूनी रूप से अस्पष्ट क्षेत्रों में इसके संचालन के कारण पेगासस स्पायवेयर को वनियमति और नरिंतरति करना मुश्किल है।
 - NSO समूह और उसके ग्राहक आमतौर पर स्पायवेयर के दुरुपयोग के लिये ज़िम्मेदारी 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.



संबंधित साइबर सुरक्षा पहल क्या हैं?

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

आगे की राह

- नगरानी उपकरणों के किसी भी अनैतिक उपयोग के लिये कंपनियों को जवाबदेह ठहराने और स्वतंत्र ऑडिट की सुविधा के लिये एक अंतरराष्ट्रीय नरीक्षण 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 अंतरराष्ट्रीय 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 नगरानी 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 सविलि सेवा परीक्षा, वगित वर्ष प्रश्न

??????:

प्रश्न1. 'वान्नाकार्ई, पेट्या और इंटरनलब्लू' पद जो हाल ही में समाचारों में उल्लिखित थे, नमिनलखिति में से कसिके साथ संबंधित हैं? (2018)

- (a) एक्सोप्लैनेट्स
- (b) प्रचछन्न मुद्रा (क्रपिटोकर्सैसी)
- (c) साइबर आक्रमण
- (d) लघु उपग्रह

उत्तर: (c)

प्रश्न2. भारत में, कसिी व्यक्तिके साइबर बीमा कराने पर नधिकी हानिकी भरपाई एवं अन्य लाभों के अतरिकित सामान्यत: नमिनलखिति में से कौन-कौन से लाभ दयि जाते हैं? (2020)

1. यदिकोई मालवेयर कंप्यूटर तक उसकी पहुँच बाधति कर देता है, तो कंप्यूटर प्रणाली को पुन: प्रचालति करने में लगने वाली लागत।
2. यदियह प्रामाणति हो जाता है किकिसी शरारती तत्त्व द्वारा जान-बूझकर कंप्यूटर को नुकसान पहुँचाया गया है तो नए कंप्यूटर की लागत।
3. यदिसाइबर बलात्-ग्रहण होता है तो इस हानिको न्यूनतम करने के लयि वशिषज्ज परामर्शदाता की सेवाएँ लेने पर लगने वाली लागत।
4. यदिकोई 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)

प्रश्न1. भारत में, साइबर सुरक्षा घटनाओं पर रिपोर्ट करना नमिनलखिति में से कसिके/कनिके लयि वधिति: अधदिशात्मक है/है? (2017)

- 1- सेवा प्रदाता (सर्विस प्रोवाइडर)
- 2- डेटा सेंटर
- 3- कॉर्पोरेट नकिय 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 वभिन्न तत्त्व क्या हैं? साइबर सुरक्षा में चुनौतयिों को धयान 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.drishtias.com/hindi/printpdf/pegasus-spyware-2>

