

राज्य प्रायोजित साइबर हमले

प्रलम्बिस के लयि:

राज्य प्रायोजित हमले, [पेगासस सपाइवेयर](#), साइबर हमला, गोपनीयता उल्लंघन, [भारतीय साइबर अपराध समन्वय केंद्र \(I4C\)](#), [साइबर सुरक्षा](#)

मेन्स के लयि:

पेगासस परयोजना और नगरानी में सुधार की आवश्यकता, सरकारी नीतियों और वभिन्न क्षेत्रों में विकास के लयि हस्तक्षेप और उनके डिज़ाइन एवं कार्यान्वयन से उत्पन्न होने वाले मुद्दे

[स्रोत: द हट्टि](#)

चर्चा में क्यों?

हाल ही में Apple Inc. ने वपिक्षी नेताओं और पत्रकारों सहति व्यक्तियों को "राज्य-प्रायोजित हमलावरों के बारे में सूचति कथिा, जो उनके iPhones को दूरस्थ गतविधियों के तहत **जोखमि में डालने की कोशशि कर रहे हैं**" ।

- ऐसा दूसरी बार हुआ है कि भारत में वपिक्षी राजनेताओं और नागरकि समाज के अभकिर्त्ताओं को चेतावनी दी गई है कि **वेजासूसी के परयासों का नशाना बने हैं** ।
- वर्ष 2021 में पेरसि स्थति [\[?/?/?/?/?/?\]](#) [\[?/?/?/?/?/?\]](#) [\[?/?/?/?/?/?\]](#) ने बताया कि [पेगासस सपाइवेयर](#), जो केवल इज़रायली फर्म NSO ग्रुप द्वारा सरकारी एजेंसियों को बेचा गया था, का कथति तौर पर भारत में कई पत्रकारों, नागरकि समाज समूहों और राजनेताओं पर इस्तेमाल कथिा गया था ।

नोट: [साइबर हमला](#) कंप्यूटर ससि्टम, नेटवर्क या डिजिटल उपकरणों की सुरक्षा में संध लगाने का एक दुर्भावनापूर्ण और जान-बूझकर कथिा गया परयास है, जसिका उद्देश्य संवेदनशील डेटा को चुराना, नुकसान पहुँचाना, बदलना या उस तक पहुँचाना, संचालन में बाधा डालना या डिजिटल क्षेत्र में नुकसान पहुँचाना है ।

राज्य प्रायोजित साइबर हमले:

- **परचिय:**
 - राज्य-प्रायोजित साइबर हमले, जनिहें राष्ट्र-राज्य साइबर हमलों के रूप में भी जाना जाता है, **अन्य देशों, संगठनों या व्यक्तियों के खिलाफ सरकारों या सरकारी एजेंसियों द्वारा संचालति या समर्थति साइबर हमले हैं** ।
 - चूँकि ये हमले कसिी राष्ट्र-राज्य के वशाल संसाधनों और क्षमताओं द्वारा समर्थति होते हैं, इसलयि वे **अपने उच्च स्तर के संगठन, जटलिता और संसाधनशीलता से प्रतषिठति होते हैं** ।
 - राज्य-प्रायोजित साइबर हमलों के उदाहरणों में स्टक्सनेट वरम शामिल है, **जसिने ईरान के परमाणु कार्यक्रम को लक्षति कथिा, वर्ष 2016 के अमेरिकी राष्ट्रपति चुनाव में कथति रूसी हस्तक्षेप** एवं वर्ष 2017 वानाक्राई रैनसमवेयर हमला, जो उत्तर कोरयिा से जुड़ा था ।
- **राष्ट्रीय सुरक्षा पर प्रभाव:**
 - **डेटा चोरी:** राज्य-प्रायोजित हमलों से संवेदनशील राष्ट्रीय सुरक्षा जानकारी, गोपनीय सैन्य सूचना और महत्त्वपूर्ण बुनयिादी ढाँचा संबंधी डेटा की चोरी हो सकती है । इस तरह के उल्लंघन कसिी देश की रक्षा क्षमताओं से समझौता कर सकते हैं ।
 - **आर्थकि प्रभाव:** प्रमुख उद्योगों और महत्त्वपूर्ण बुनयिादी ढाँचे पर हमलों से आर्थकि नुकसान हो सकता है । उदाहरण के लयि ऊर्जा या वत्तितीय प्रणालियों में व्यवधान के गंभीर आर्थकि परिणाम हो सकते हैं ।
 - **राजनीतकि प्रभाव:** साइबर हमलों का उपयोग जनता की राय में हेर-फेर करने, चुनावों को प्रभावति करने और राजनीतकि स्थरिता को कमज़ोर करने के लयि कथिा जा सकता है । दुष्प्रचार अभयान तथा हैककि के दूरगामी राजनीतकि प्रभाव हो सकते हैं ।

- राष्ट्रीय संप्रभुता: साइबर हमले किसी देश की संप्रभुता का उल्लंघन कर सकते हैं और अपने नागरिकों पर शासन करने तथा उनकी रक्षा करने की क्षमता से समझौता कर सकते हैं।

?????? (Pegasus):

■ परिचय:

- यह एक प्रकार का मैलेशियस सॉफ्टवेयर या मैलवेयर है जिसे स्पाइवेयर के रूप में वर्गीकृत किया गया है।
 - यह उपयोगकर्ताओं की जानकारी के बिना उपकरणों तक पहुँच प्राप्त करने के लिये डिज़ाइन किया गया है और व्यक्तिगत जानकारी एकत्र करता है तथा इसे वापस रलि करने के लिये सॉफ्टवेयर का उपयोग किया जाता है।
- पेगासस को इज़रायली फर्म NSO ग्रुप द्वारा विकसित किया गया है जिस वर्ष 2010 में स्थापित किया गया था।
 - पेगासस संक्रमण को ऑपरेटिंग सिस्टम की खामियों का फायदा उठाकर तथाकथित "ज़ीरो-क्लिक" हमलों के माध्यम से प्राप्त किया जा सकता है, जिसके सफल होने के लिये फोन के मालिक से किसी भी बातचीत की आवश्यकता नहीं होती है।

■ लक्ष्य:

- इज़रायल की नगरानी वाली फर्म द्वारा सत्तावादी सरकारों को बेचे गए एक फोन मैलवेयर के माध्यम से दुनिया भर के मानवाधिकार कार्यकर्ताओं, पत्रकारों और वकीलों को लक्षित किया गया है।
- भारतीय मंत्री, सरकारी अधिकारी और वपिक्षी नेता भी उन लोगों की सूची में शामिल हैं जिनके फोन पर इस स्पाइवेयर द्वारा छेड़छाड़ किये जाने की संभावना व्यक्त की गई है।
 - वर्ष 2019 में व्हाट्सएप ने इज़रायल के NSO ग्रुप के खिलाफ अमेरिकी न्यायालय में एक मुकदमा दायर किया, जिसमें आरोप लगाया गया था कि यह फर्म मोबाइल उपकरणों को दुर्भावनापूर्ण सॉफ्टवेयर से संक्रमित करके एप्लीकेशन पर साइबर हमलों को प्रेरित कर रही है।

■ साइबर सुरक्षा हेतु पहलें:

- भारतीय पहलें:
 - साइबर सुरक्षा भारत पहल
 - राष्ट्रीय साइबर सुरक्षा समन्वय केंद्र (NCCC)
 - साइबर स्वच्छता केंद्र
 - भारतीय साइबर अपराध समन्वय केंद्र (I4C)
 - भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया टीम, सर्ट-इन (Indian Computer Emergency Response Team- CERT-In)
- वैश्विक पहलें:
 - अंतरराष्ट्रीय दूरसंचार संघ (ITU)
 - साइबर अपराध पर बुडापेस्ट अभिसमय

आगे की राह

- व्यापक राष्ट्रीय साइबर सुरक्षा नीतियों और रणनीतियों को विकसित करने तथा लागू करने की आवश्यकता है जो साइबर क्षेत्र में रक्षा एवं अपराध दोनों का समाधान करेंगी।
- सरकारी एजेंसियों के लिये घुसपैठ पहचान हेतु उन्नत प्रणाली, सुरक्षित नेटवर्क और साइबर सुरक्षा प्रशिक्षण सहित साइबर सुरक्षा बुनियादी ढाँचे को मज़बूत करने के लिये संसाधन आवंटित करने की आवश्यकता है।
- खतरे की खुफिया जानकारी साझा करने और राज्य-प्रायोजित खतरों पर प्रतिक्रियाओं का समन्वय करने के लिये अन्य देशों तथा अंतरराष्ट्रीय संगठनों के साथ सहयोग करना चाहिये।