समाचार वाणी
ख़बर जो करें असर !

नाशिक | Wednesday, 23 September 2026

पेगासस के बाद 'पैरागॉन' ने मचाई सनसनी, जासूसी के नए हथियार से हिली दुनियाभर की सरकारें

Publisher

Published on 10 Oct 2025

पेगासस जासूसी कांड के बाद अब दुनिया के सामने एक नया खतरा खड़ा हो गया है — **'पैरागॉन स्पाईवेयर' (Paragon Spyware)**। यह नया साइबर हथियार दुनिया के कई देशों की सुरक्षा एजेंसियों और उच्च पदस्थ अधिकारियों के फोन में घुसपैठ करने की क्षमता रखता है। हाल के दिनों में इसके इस्तेमाल के कई चौंकाने वाले मामले सामने आए हैं, जिससे साइबर सुरक्षा एजेंसियों में हड़कंप मच गया है।

सूत्रों के अनुसार, पैरागॉन का उपयोग कई देशों में **राजनीतिक जासूसी**, **राजनयिक निगरानी** और **मीडिया व्यक्तित्वों की ट्रैकिंग** के लिए किया जा रहा है। इस सॉफ्टवेयर की क्षमताएं पेगासस से भी अधिक उन्नत बताई जा रही हैं, जो इसे और अधिक खतरनाक बनाती हैं।

जैसे पेगासस बिना किसी लिंक पर क्लिक किए ही मोबाइल में घुस जाता था, वैसे ही पैरागॉन भी '**जीरो-क्लिक एक्सप्लॉइट**' का उपयोग करता है। इसका मतलब यह है कि पीड़ित व्यक्ति को किसी लिंक या फाइल पर क्लिक करने की आवश्यकता नहीं होती, फिर भी यह स्पाईवेयर उसके फोन में इंस्टॉल हो सकता है।

साइबर विशेषज्ञों का कहना है कि पैरागॉन में एंड्रॉइड और iOS दोनों सिस्टम को **रूट एक्सेस** मिल जाता है, जिससे यूजर की हर गतिविधि पर नजर रखी जा सकती है। फोन कॉल्स, मैसेज, ईमेल, फोटो, लोकेशन — सब कुछ पैरागॉन के सर्वर तक पहुंच जाता है।

यहां तक कि यह स्पाईवेयर मोबाइल के कैमरे और माइक्रोफोन को **रिमोटली एक्टिवेट** कर सकता है, जिससे यूजर की निजी बातचीत और वीडियो रिकॉर्डिंग तक संभव हो जाती है।

पेगासस की तुलना में पैरागॉन को ज्यादा एडवांस माना जा रहा है। पेगासस मुख्य रूप से iPhone यूजर्स को टारगेट करता था,

जबकि पैरागॉन सभी ऑपरेटिंग सिस्टम्स पर काम कर सकता है।

रिपोर्ट्स के मुताबिक, पैरागॉन डेटा चोरी करने के अलावा उसे **एन्क्रिप्टेड नेटवर्क्स से बाहर निकालने की क्षमता** रखता है, यानी यह WhatsApp, Signal या Telegram जैसी सुरक्षित मैसेजिंग ऐप्स में हो रही बातचीत को भी पकड़ सकता है।

साइबर सुरक्षा फर्मों का कहना है कि पैरागॉन को "नेक्स्ट जनरेशन डिजिटल सर्विलांस सिस्टम" के रूप में डिजाइन किया गया है, जिसका मकसद सिर्फ जासूसी ही नहीं बल्कि डेटा मॉडिफिकेशन तक हो सकता है।

अंतरराष्ट्रीय मीडिया रिपोर्ट्स के अनुसार, पैरागॉन स्पाईवेयर के सर्वर कई देशों में फैले हुए हैं, जिनमें **अमेरिका, इज़रायल, फ्रांस, जर्मनी, भारत, और सऊदी अरब** जैसे देश शामिल हैं।
विशेषज्ञों का अनुमान है कि यह स्पाईवेयर सरकारी एजेंसियों को "**क्लाउड बेस्ड मॉनिटरिंग एक्सेस**" उपलब्ध कराता है, जिससे वे बिना किसी भौतिक हस्तक्षेप के टारगेट की जासूसी कर सकें।

हालांकि अभी तक यह स्पष्ट नहीं हो पाया है कि इस स्पाईवेयर को किस कंपनी या देश ने विकसित किया है, लेकिन इसके **स्रोत को इज़रायल की एक टेक कंपनी से जुड़ा बताया जा रहा है**, जिसने पहले भी सुरक्षा और निगरानी से जुड़े टूल्स बनाए हैं।

प्रारंभिक जांच से पता चला है कि पैरागॉन के जरिए मुख्य रूप से **पत्रकारों, मानवाधिकार कार्यकर्ताओं, विपक्षी नेताओं और उद्योगपतियों** को निशाना बनाया गया है।
कई अंतरराष्ट्रीय मीडिया संस्थानों ने खुलासा किया है कि इस स्पाईवेयर के जरिए **कूटनीतिक वार्ताओं और सरकारी गोपनीय बैठकों** की जासूसी की गई है।

भारत में भी कुछ साइबर सुरक्षा विशेषज्ञों ने इस पर चिंता जताई है। उनका कहना है कि देश को इस तरह के अत्याधुनिक साइबर हथियारों से निपटने के लिए एक **राष्ट्रीय साइबर सुरक्षा नीति** की जरूरत है, जो तकनीकी रूप से सक्षम हो।

पैरागॉन को इस तरह डिजाइन किया गया है कि इसे **ट्रैक करना लगभग असंभव** है। यह अपने निशान मिटा देता है और किसी भी सिक्योरिटी स्कैनर में दिखाई नहीं देता।
यह फोन के ऑपरेटिंग सिस्टम की मूल परतों तक पहुंच जाता है और वहां से डेटा कलेक्ट करता है। यही कारण है कि सामान्य एंटीवायरस सॉफ्टवेयर इसे पकड़ नहीं पाते।

साइबर विशेषज्ञों का कहना है कि यह स्पाईवेयर इतना एडवांस है कि यह खुद को सिस्टम अपडेट्स के साथ एडजस्ट कर लेता है, यानी कंपनी जब भी नया सिक्योरिटी पैच जारी करती है, पैरागॉन खुद को उसके अनुसार बदल लेता है।

पैरागॉन के खुलासे के बाद कई देशों की सरकारों ने इसकी जांच शुरू कर दी है। यूरोपियन यूनियन ने इस मामले पर साइबर सुरक्षा आयोग की विशेष बैठक बुलाई है। वहीं अमेरिका ने अपने नागरिकों की डिजिटल प्राइवेसी की सुरक्षा के लिए नए दिशानिर्देश जारी किए हैं।

संयुक्त राष्ट्र के मानवाधिकार विशेषज्ञों ने भी चिंता जताई है कि इस तरह के स्पाईवेयर लोकतंत्र और अभिव्यक्ति की स्वतंत्रता के लिए **गंभीर खतरा** बन सकते हैं। उन्होंने तकनीकी कंपनियों से कहा है कि वे ऐसे उपकरणों के खिलाफ एकजुट होकर काम करें।

भारत में पेगासस कांड के बाद से डिजिटल निगरानी को लेकर बहस तेज हो गई थी। अब पैरागॉन के खुलासे ने इस बहस को और हवा दे दी है। साइबर एक्सपर्ट्स का कहना है कि भारत जैसे विशाल डिजिटल इकोसिस्टम वाले देश में अगर यह स्पाईवेयर फैलता है तो **राष्ट्रीय सुरक्षा, आर्थिक डेटा और नागरिकों की निजता** सभी पर खतरा मंडरा सकता है।

भारतीय सरकार ने अब तक इस पर कोई आधिकारिक बयान जारी नहीं किया है, लेकिन गृह मंत्रालय और आईटी विभाग ने इसे लेकर प्रारंभिक जानकारी जुटानी शुरू कर दी है।

पेगासस के बाद पैरागॉन का सामने आना इस बात का संकेत है कि **साइबर जासूसी का युग अब और भी खतरनाक रूप ले चुका है**। जहां पहले फोन कॉल या मैसेज तक सीमित निगरानी होती थी, अब तकनीक इतनी उन्नत हो गई है कि व्यक्ति के पूरे डिजिटल जीवन पर नजर रखी जा सकती है।