पेगासस : तकनीक और जासूसी

(प्रारंभिक परीक्षा- राष्ट्रीय और अंतर्राष्ट्रीय महत्त्व की सामयिक घटनाएँ, सामान्य विज्ञान)
(मुख्य परीक्षा, सामान्य अध्ययन प्रश्नपत्र- 3 : सूचना प्रौद्योगिकी, संचार नेटवर्क के माध्यम से आंतरिक सुरक्षा को चुनौती, आंतरिक सुरक्षा चुनौतियों में मीडिया और सामाजिक नेटवर्किंग साइटों की भूमिका, साइबर सुरक्षा की बुनियादी बातें, धन-शोधन और इसे रोकना)

संदर्भ

हाल ही में, पत्रकारों के एक अंतर्राष्ट्रीय समूह ने इज़रायली कंपनी एन.एस.ओ. (NSO) के जासूसी सॉफ्टवेयर 'पेगासस' (Pegasus) से मंत्रियों, विपक्ष के नेता, पत्रकार, अधिवक्ता, न्यायाधीश, उद्योग जगत के लोग, अधिकारी, वैज्ञानिक और कार्यकर्त्ताओं की जासूसी का दावा किया है। इस अंतर्राष्ट्रीय समूह में 17 मीडिया संस्थान और एमनेस्टी इंटरनेशनल शामिल हैं।

क्या है पेगासस प्रोजेक्ट?

- 'पेगासस प्रोजेक्ट' दुनियाभर के 17 मीडिया संस्थानों के पत्रकारों का एक समूह है, जो एन.एस.ओ. (NSO) समूह और उसके सरकारी ग्राहकों की जाँच कर रहा है। एन.एस.ओ. एक इज़रायली कंपनी है, जो सरकारों को सर्विलांस तकनीक बेचती है।
- 'पेगासस' इसके प्रमुख उत्पादों में से एक है, जोकि एक 'जासूसी सॉफ्टवेयर' या 'स्पाइवेयर' है। यह आईफोन और एंड्रॉयड डिवाइस को लक्षित करता है और इंस्टॉल होने पर फोन से चैट, फोटो, ईमेल और लोकेशन डाटा ले सकता है। डिवाइस के उपयोगकर्ता को इसकी जानकारी भी नहीं हो पाती है और यह फोन का माइक्रोफोन व कैमरा सक्रिय कर देता है।
- फ्रांस स्थित गैर-लाभकारी पत्रकारिता समूह 'फॉरबिडन स्टोरीज़' और 'एमनेस्टी इंटरनेशनल' के पास वर्ष 2016 से एन.एस.ओ. के ग्राहकों (सरकारों) द्वारा लक्षित फोन नंबरों की जानकारी पहुँची। इसको उसने गार्जियन, वॉशिंगटन पोस्ट सहित 10 देशों के 17 समाचार संगठनों (मीडिया संस्थानों) से साझा किया। इन संस्थानों के बीच समन्वय का कार्य फॉरबिडन स्टोरीज करता था।
- लक्षित नंबरों में से कुछ लोगों के मोबाइल हैंडसेटो की फोरेंसिक जांच एमनेस्टी की सिक्योरिटी लैब (सिटिजन लैब) से कराई गई, जो इस प्रोजेक्ट में तकनीकी सहायक बने।

एन.एस.ओ. और पेगासस

- एन.एस.ओ. या क्यू साइबर टेक्नोलॉजी समूह इज़रायल की एक निजी कंपनी है। यह दुनिया के उच्चस्तर के स्पाइवेयर बनाने में सक्षम है। 'पेगासस' इसका सबसे चर्चित उत्पाद है, जिसे आईफोन और एंड्रॉयड डिवाइस में सेंधमारी के लिये डिज़ाइन किया गया है। पेगासस का दूसरा नाम 'क्यू सुइट' भी है।
- इस कंपनी की स्थापना वर्ष 2010 में हुई थी। इज़रायल के अतिरिक्त इस कंपनी का बुल्गारिया और साइप्रस में भी कार्यालय है। इस कंपनी की मेजॉरिटी ओनरशिप लंदन की प्राइवेट इक्विटी फर्म 'नोवाल्पिना कैपिटल' के पास है।
- सिटिजन लैब के अनुसार, पेगासस से जुड़े 45 देशों के डॉक्यूमेंट हैं। इनमें अल्जीरिया, बहरीन, बांगलादेश, ब्राजील, कनाडा, केन्या, कुवैत, किर्गिस्तान, लातविया व लेबनान के साथ-साथ लीबिया, मैक्सिको, मोरक्को, नीदरलैंड, ओमान, पाकिस्तान, फिलिस्तीन, पोलैंड, कतर, रवांडा, सऊदी अरब, सिंगापुर तथा दक्षिण अफ्रीका, स्विट्जरलैंड, यूनाइटेड किंगडम व अमेरिका जैसे देश शामिल हैं।
- उल्लेखनीय है कि वर्ष 2019 में वॉट्सअप ने पेगासस की निर्माता कंपनी पर मुकदमा भी किया था। वर्ष 2019 में जब वॉट्सअप के माध्यम से डिवाइसेस में पेगासस इंस्टॉल किया गया था तब हैकर्स ने वॉट्सअप के वीडियो कॉल फीचर में एक कमी (बग) का लाभ उठाया था।
- ग्रीक की पौराणिक कथाओं में पेगासस का अर्थ 'पंखों वाला घोड़ा' होता है। इसने अपनी कंपनी का लोगो भी इसी काल्पनिक घोड़े के आधार पर बनाया है।

स्पाइवेयर

'स्पाइवेयर' किसी की जासूसी कराने के लिये तैयार किया गया सॉफ्टवेयर या मालवेयर होता है। इनका प्रयोग कंप्यूटर, मोबाइल या किसी दूसरे डिवाइस से जानकारी एकत्रित करने के लिये किया जाता है।

पेगासस जैसे स्पाइवेयर और चुराई जा सकने वाली जानकारियाँ

- एक परिष्कृत सॉफ्टवेयर (स्पाइवेयर) डिवाइस में मौजूद लगभग हर जानकारी को चुरा सकता है। यह रियल टाइम फोन कॉल को सुन सकता है। साथ ही, ईमेल, सोशल मीडिया पोस्ट, कॉल लॉग, वॉट्सएप या टेलीग्राम जैसे एंड टु एंड एन्क्रिप्टेड मैसेज को भी पढ़ सकता है।
- यह उपयोगकर्ता की लोकेशन के साथ यह भी पता लगा सकता है कि वह कितनी गति से और किस दिशा में चल रहा या रुका हुआ है। यह फोन या सिम से कॉन्टैक्ट, यूजर नेम, पासवर्ड, नोट्स और डॉक्यूमेंटस के अतिरिक्त फोटो, वीडियो और साउंड रिकॉर्डिंग, एस.एम.एस., नेटवर्क डिटेल्स, डिवाइस सेटिंग, ब्राउजिंग हिस्ट्री की जानकारी भी एकत्रित कर सकता है।
- यह स्पाइवेयर स्मार्ट फोन या स्मार्ट डिवाइस के कैमरे और माइक्रोफोन भी चालू (ऑन) कर सकता है। कुछ स्पाइवेयर बिना पता लगे दूसरे डिवाइस को फाइल भी भेज सकते हैं।
- इंस्टॉल होने के बाद पेगासस फोन में किसी तरह के फुटप्रिंट नहीं छोड़ता है, अर्थात फोन हैक होने पर भी पता नहीं चलता है। यह कम बैंडविड्थ पर भी कार्य कर सकता है। साथ ही, बैटरी, मेमोरी व डाटा का भी कम उपयोग करता है, जिससे फोन हैक होने पर कोई संदेह न हो।

मोबाइल में स्पाइवेयर पहचानने का तरीका

- यदि मोबाइल अनपेक्षित व्यवहार करने लगे तो वह स्पाइवेयर से इंफेक्ट हो सकता है। इस अनपेक्षित व्यवहार में मोबाइल का तेजी से गर्म होना, मेमोरी का करप्ट होना, वॉट्सअप या टेलीग्राम के मैसेज का अचानक डिलीट होने लगना शामिल है।

- पेगासस एक अत्याधुनिक स्पाइवेयर है। ऐसे टूल्स की पहचान के लिये फोरेंसिक विश्लेषण की आवश्यकता होती है और टूलकिट से जाँच की जाती है। एमनेस्टी इंटरनेशनल का 'मोबाइल वेरिफिकेशन टूलकिट' (MVT) इसे डिटेक्ट करने में मदद कर सकता है।

क्या होता है जीरो क्लिक अटैक?

- पैगासस स्पाइवेयर स्मार्टफोन या स्मार्ट डिवाइस में सेंधमारी के लिये 'फिशिंग मैसेज' (जैसे- लिंक या मैसेज भेजना) का सहारा नहीं लेता है। पैगासस का आधुनिक अटैक डिवाइस पर कोई लिंक या मैसेज नहीं भेजता, जिस पर क्लिक करने से मेलवेयर डिवाइस में फैल सके।
- पैगासस को स्पाइवेयर के नए तरीके में डिवाइस उपयोगकर्ता के किसी प्रतिक्रिया (एक्शन) की आवश्यकता ही नहीं होती है। अर्थात उपयोगकर्ता को किसी प्रकार की मिस क़ॉल, मैसेज या किसी तरह की कोई लिंक नहीं आता (जिस पर क्लिक या प्रतिक्रिया करने की आवश्यकता हो) है।
- स्पाइवेयर से अटैक की इसी तकनीक को 'ज़ीरो क्लिक अटैक' कहते हैं। वर्ष 2019 में गूगल के प्रोजेक्ट ज़ीरो सिक्योरिटी रिसर्चर इयान बीयर ने दिखाया कि अटैकर ने किसी लिंक आदि पर क्लिक कराए बिना ही 'रेडियो प्रॉक्सिमिटी' के जरिये उनके आईफोन को पूरी तरह अपने नियंत्रण में ले लिया।

स्पाइवेयर और कुछ सुरक्षा उपाय

- सभी डिवाइस और सॉफ्टवेयर को अप-टु-डेट रखना चाहिये, जिसके लिये सेटिंग में 'ऑटोमैटिक अपडेट्स' को सक्रिय करना चाहिये।
- अधिक पुराने डिवाइस पर ऐसे स्पाइवेयर हमलों का शिकार बनने का जोखिम अधिक होता है। विशेषकर यदि वे पुराने ऑपरेटिंग सिस्टम पर चल रहे हों।
- डिवाइस, साइट और ऐप के लिये अद्वितीय पासवर्ड की आवश्यकता होती है। फोन नंबर, जन्मतिथि आदि के आधार पर रखे गए पासवर्ड को हैक करना सरल होता है और पासवर्ड मैनेजर, जैसे 'लास्टपास' या 'वन पासवर्ड' इसको आसान बना सकते हैं।
- इसके अतिरिक्त, जहाँ तक संभव हो 'टू फैक्टर ऑथेंटिकेशन' (Two-Factor Authentication) को सक्रिय कर देना चाहिये। ऐसी साइट्स पासवर्ड के साथ-साथ दूसरा कोड भी मांगती है।
- अनजान लिंक या अटैचमेंट पर क्लिक नहीं करना चाहिये।
- साथ ही, 'डिसअपियरिंग मैसेज' (Disappearing Messages) या ऐसी दूसरी सेटिंग को सक्रिय कर देना चाहिये, जिससे एक निश्चित समय के बाद मैसेज या दूसरे कम्युनिकेशन स्वत: गायब हो जाएँ।

सर्विलांस और कानून

- भारत में 'आई.टी. अधिनियम, 2000' की धारा 69 और 'टेलीग्राफ अधिनियम, 1985' की धारा 5 सरकार को सर्विलांस का अधिकार देती है किंतु इसके लिये देश की संप्रभुता, अखंडता व सुरक्षा जैसे आधार जरूरी हैं। देश में निजी सर्विलांस की कोई अनुमति नहीं है।
- इसी तरह आई.टी. अधिनियम की धारा 43 और धारा 66 के तहत हैंकिंग पूर्णतया प्रतिबंधित है। इस अधिनियम की धारा 66B के तहत कंप्यूटर या अन्य किसी इलेक्ट्रॉनिक गैजेट से चोरी की गई सूचनाओं को गलत तरीके से प्राप्त करने पर तीन वर्ष तक कारावास हो सकता है।