मर्सेनरी स्पाईवेयर हमला

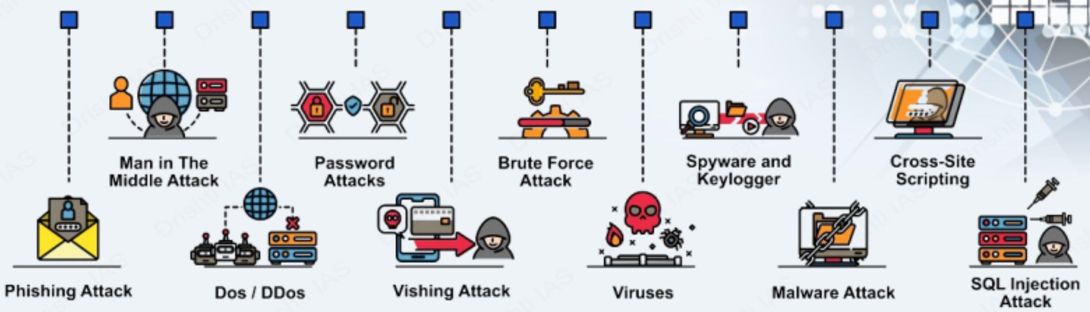
Apple ने हाल ही में भारत और 91 अन्य देशों में **iPhone** उपयोगकर्त्ताओं के लिये तत्काल सुरक्षा अलर्ट जारी किया है। अधिसूचनाओं में चेतावनी दी गई है कि उनके उपकरणों को **मर्सेनरी स्पाईवेयर हमले (mercenary spyware attack)** में दूर से निशाना बनाया गया है।

- नियमित **साइबर आपराधिक गतिविधि** या उपभोक्ता मैलवेयर की तुलना में मर्सेनरी स्पाइवेयर हमले असाधारण रूप से दुर्लभ और अत्यधिक परिष्कृत होते हैं।
- आम साइबर खतरों के विपरीत, **मर्सेनरी स्पाईवेयर हमले** का उद्देश्य उपयोगकर्त्ता के डिवाइस तक **अनधिकृत पहुँच** प्राप्त करना है।
  - यदि किसी डिवाइस पर लक्षित मर्सेनरी स्पाईवेयर हमले से छेड़छाड़ की जाती है, तो हमलावर **संवेदनशील डेटा**, संचार या यहाँ तक कि कैमरा और माइक्रोफोन तक दूरस्थ रूप से पहुँचने में सक्षम हो सकता है।
  - ये **रणनीतिक रूप से लक्षित**, उच्च लागत वाले हमले हैं, जो ऐतिहासिक रूप से राज्यों से जुड़े हुए हैं, पत्रकारों, कार्यकर्त्ताओं, राजनेताओं और राजनयिकों जैसे चुनिंदा व्यक्तियों को लक्षित करते हैं।
  - NSO ग्रुप द्वारा विकसित पेगासस**, मर्सनिरी स्पाइवेयर के उदाहरणों में से एक है।**

साइबर सुरक्षा

साइबर सुरक्षा, साइबर हमलों को रोकने या उनके प्रभाव को कम करने के लिये किसी भी तकनीक, उपाय या अभ्यास को संदर्भित करती है।

CYBER SECURITY ATTACKS



NCRB की "भारत में अपराध" रिपोर्ट, 2022 के अनुसार, वर्ष 2021 के बाद से भारत में साइबर अपराध 24.4% बढ़ गए हैं।

सामान्य साइबर सुरक्षा मिथक

- केवल मज़बूत पासवर्ड ही पर्याप्त सुरक्षा है
- प्रमुख साइबर सुरक्षा जोखिम सर्वविदित हैं
- सभी साइबर हमले वैक्टर (vector) निहित होते हैं
- साइबर अपराधी छोटे व्यवसायों पर हमला नहीं करते हैं

साइबर वॉर

- किसी दूसरे के कंप्यूटर सिस्टम को बाधित करने, क्षति पहुँचाने या नष्ट करने के लिये किये गए डिजिटल हमले।

CYBER THREAT ACTORS

CYBER THREAT ACTOR	MOTIVATION
NATION-STATES	GEOPOLITICAL
CYBERCRIMINALS	PROFIT
HACKTIVISTS	IDEOLOGICAL
TERRORIST GROUPS	IDEOLOGICAL VIOLENCE
THRILL-SEEKERS	SATISFACTION
INSIDER THREATS	DISCONTENT

साइबर सुरक्षा के प्रकार

- महत्त्वपूर्ण बुनियादी ढाँचा सुरक्षा (रोबस्ट एक्सेस कंट्रोल)
- नेटवर्क सुरक्षा (डिप्लॉयिंग फायरवॉल)
- एप्लिकेशन सुरक्षा (कोड रिव्यु)
- क्लाउड सुरक्षा (टोकनाइज़ेशन)
- सूचना सुरक्षा (डेटा मास्किंग)

हाल ही में हुए प्रमुख साइबर हमले

- वान्नाक्राई रैनसमवेयर अटैक (वर्ष 2017)
- कैम्ब्रिज एनालिटिका डेटा ब्रीच (वर्ष 2018)
- 9M+ कार्डधारकों का वित्तीय डेटा लीक, जिसमें SBI भी शामिल है (वर्ष 2022)

विनियम एवं पहलें

- **अंतर्राष्ट्रीय स्तर पर:**
  - साइबर स्पेस में राज्यों के उत्तरदायी व्यवहार को बढ़ावा देने से संबंधित संयुक्त राष्ट्र के सरकारी विशेषज्ञों के समूह (GGE)।
  - नाटो का कोऑपरेटिव साइबर डिफेंस सेंटर ऑफ एक्सीलेंस (CCDCOE)
  - साइबर अपराध पर बुडापेस्ट कन्वेंशन, 2001 (भारत हस्ताक्षरकर्त्ता नहीं है)
- **भारतीय स्तर पर:**
  - IT अधिनियम, 2000 (धारा 43, 66, 66B, 66C, 66D)
  - राष्ट्रीय साइबर सुरक्षा नीति, 2013
  - नेशनल साइबर सिक्योरिटी स्ट्रेटेजी, 2020
  - साइबर सुरक्षित भारत पहल
  - भारतीय साइबर अपराध समन्वय केंद्र (I4C)
  - कंप्यूटर आपातकालीन प्रतिक्रिया टीम - भारत (CERT-In)

साइबर सुरक्षा के लिये उठाए जाने वाले आवश्यक कदम

- नेटवर्क सुरक्षा
- मैलवेयर सुरक्षा
- इंसिडेंट मैनेजमेंट
- उपयोगकर्त्ता को शिक्षित और जागरूक करना
- सुरक्षित विन्यास
- उपयोगकर्त्ता के विशेषाधिकारों का प्रबंधन करना
- सूचना जोखिम प्रबंधन व्यवस्था

Drishti IAS

//

और पढ़ें: [पेगासस स्पाईवेयर]

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/mercenary-spyware-attack