DDoS साइबर अटैक

स्रोत: TH

संपत्ति पंजीकरण से संबंधित कर्नाटक के कावेरी 2.0 पोर्टल को डिस्ट्रीब्यूटेड डेनियल ऑफ सर्विस (DDoS) अटैक के कारण उत्पन्न समस्याओं का सामना करना पड़ा।

- **स्वचालित अनुरोधों और फेक एकाउंट्स के कारण सिस्टम पर अत्यधिक बोझ पड़ने से डाउनटाइम की समस्या उत्पन्न हो गई।**
- **डिस्ट्रीब्यूटेड डेनियल ऑफ सर्विस (DDoS) अटैक:**
- **DDoS अटैक** एक **साइबर** अटैक है, जिसमें दुर्भावनापूर्ण ट्रैफिक किसी नेटवर्क या वेबसाइट पर अत्यधिक भार डाल देता है, जिससे कार्य बाधित होता है।
- **DDoS** अटैक, **डेनियल ऑफ सर्विस (DoS) हमलों का बड़े** पैमाने का संस्करण हैं, जो **लक्ष्य को अधिभारित करने** के लिये एकल स्रोत के बजाय **कई समझौता किये गए सिस्टम (बॉटनेट)** का उपयोग करते हैं।
- **प्रकार:**

//

विभिन्न प्रकार के DDoS अटैक

वॉल्यूम-बेज्ड अटैक

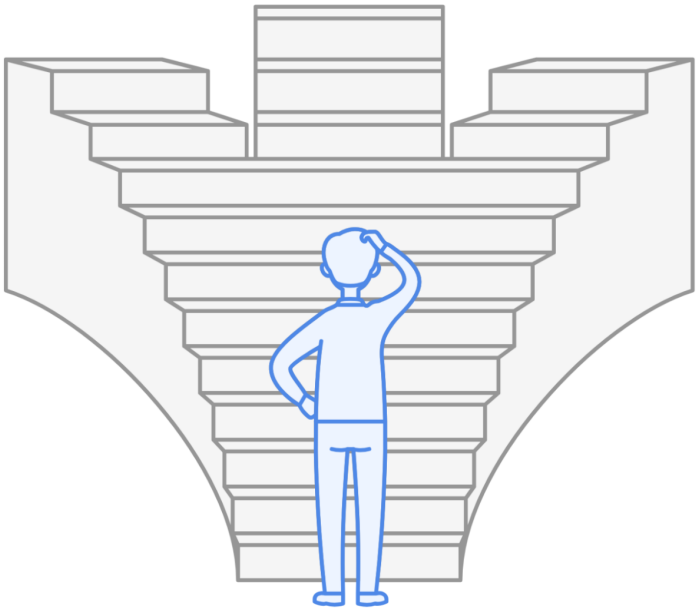
उच्च ट्रैफिक के साथ नेटवर्क बैंडविड्थ को ओवरलोड करना

प्रोटोकॉल अटैक

सर्वर संसाधनों को नष्ट करने के लिये प्रोटोकॉल की कमज़ोरियों का लाभ उठाना

एप्लिकेशन लेयर अटैक

एप्लिकेशन की गति को धीमा या क्रैश करने के लिये विशिष्ट सेवाओं को लक्षित करना

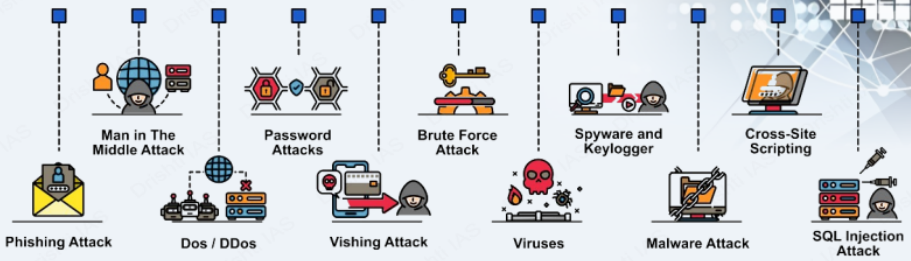


- **प्रभाव:**
- DDoS अटैक **सेवाओं को बाधति करते हैं, राजस्व को प्रभावति करते हैं,** तथा साइबर सुरक्षा कमज़ोरियों को उजागर करते हैं, जसिसे संगठन की प्रतषि्ठा को नुकसान पहुँचता है।
- **शमन संबंधी रणनीतयिाँ**
- **ट्रैफकि फलि्टरगि**, दर सीमा, सकि्यूरटिी ऑडटि, घटना प्रतकि्रयिा योजना, बहु-कारक प्रमाणीकरण और बॉट डटिेक्शन (कैप्चा, व्यवहार वशि्लेषण) द्वारा DDoS अटैक के वरिुद्ध सुरक्षा में सुधार कयिा गया 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 रिव्यू)
- 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: डिनायल ऑफ-सर्वसि (DoS) अटैक