11-03-2018

Cryptojacking

What is it?

- Cryptojacking is defined as the secret use of your computing device to mine cryptocurrency.
- Cryptojacking used to be confined to the victim unknowingly installing a program that secretly mines cryptocurrency.

About cryptojacking:

- Cryptojackers usually target popular websites which draw audiences numbering in the millions every day.
- Once the malware patch has been embedded on a website, it infects the web browsers of visitors, slowing down their machines, often causing them to overheat.
- Websites and apps which do not seemingly charge a fee for your consuming their content survive on revenue from digital advertising. However, websites like the file-sharing platform Pirate Bay have been found to be employing code which hijacks your system and uses it for mining Monero – a cryptocurrency whose value has almost increased fivefold in the past six months.
- Coinhive is a tool that allows companies to 'monetize their digital business with their users' CPU power.' The tool patches the JavaScript for the website's pages, enabling it to stealthily access the hardware of its users without their knowledge.

Who are mostly infected by cryptojacking:

- According to digital security firm Wandera, scripts like Coinhive can be embedded on to any app or website, and that users of social media platforms like Facebook, Instagram, and Pinterest are exposed to links containing malicious scripts.
- The increase in number of mobile devices which are being used to access the internet has also put a large segment of devices running on relatively open environments such as Android at risk of being infected.
- Wandera found that mobile devices that fell prey to cryptojacking websites and apps increased by 287% between October and November 2017.
- Apple's iPhones are also vulnerable to being cryptojacked.

How can computers be safeguarded from being cryptojacked:

- Here is a list of applications that could protect your computer from attacks by cryptojackers.

1. **NoCoin:**

- It is an extension that can be loaded on web browsers like Google Chrome, Mozilla Firefox, and Opera. In addition to Coinhive, it provides security against other mining software which mine for bitcoin, ethereum, and ripple. However, it also allows users to turn off protection for certain websites. NoCoin is an open source tool, the code to which is available on Github.

2. **MalwareBytes:**

- Unlike NoCoin, this a software package that acts as a bulwark against a wide variety of malware, and also hackers who try to breach private networks.The company boasts that its product detected and quarantined 1,30,000 WannaCry ransomware infections in the first week of its outbreak. MalwareBytes also allows users to remove particular domains or IP addresses from its block list.

3. **minerBlock**

- minerBlock is another anti-mining browser extension that can block cryptojacking attempts by software patches on websites.
- It maintains a blacklist of compromised websites, and lets users manually add to this list.

Expected prelims question

Cryptojacking is in news recently, it is related to

a) Malware
b) New software app
c) New form of Bitcoin
d) None of above

Ans - a

Expected mains question:

The transition to a digital economy made people mostly dependent on technology; simultaneously it has spawned a new breed of hackers.Critically Analyse the new hacking systems and also add anote on Few Important Anti Hacking systems developed to secure personal information.