Cryptojacking and Cryptocurrency Mining

What is the issue?

\n\n

\n
- The ever increasing attractiveness for cryptocurrency mining is leaving way for new threats in the cyber space.
\n
- Cryptojacking has become the latest threat to computers worldwide.
\n

\n\n

How do cryptocurrencies work?

\n\n

\n
- Cryptocurrencies like Bitcoin are based on the **blockchain technology.**
\n
- The blockchain technology involves maintaining a **digital ledger** to publicly record transactions.
\n
- A blockchain is reliant on the **network of computers** that run the software for the cryptocurrency.
\n
- The computers participate in the relay of information regarding **transactions** made between holders of the currency.
\n
- These computers in the network are called **nodes**.
\n
- They can be operated by anyone who downloads the **bitcoin software** available for free online.
\n
- When a transaction is initiated, **encrypted details** are transmitted among all nodes.
\n

\n\n

What is cryptocurrency mining?

\n\n

\n
- The money in cryptocurrency is not printed. It is rather discovered, or “mined”.
\n
- Mining is used to confirm waiting transactions and then record it into a public ledger called blockchain.
\n
- The web of nodes in blockchain technology includes those operated by **miners**.
\n
- Miners' objective is to group the outstanding transactions into blocks and then add them to the blockchain.
\n
- A mining hardware competes with others on the network to earn cryptocurrencies.
\n

\n\n

How does mining work?

\n\n

\n
- Computers around the world “Mine” for bitcoins competing with each other.
\n
- Adding encrypted transactions to the blockchain is accomplished by the miner's cryptocurrency software.
\n

\n\n

\n
- This involves solving a complex mathematical puzzle involving the numerical keys to the encryption.
\n
- Once a node has hit upon the right combination, it conveys its success to other nodes.
\n
- Subsequently, other miners drop processing that block and move on to the next.
\n

- The winning node that registers a transaction by adding it to the blockchain is rewarded in Bitcoin.
  \n

\n\n

What are the challenges?

\n\n

  \n
- The cost of mining is often highly expensive.
  \n

\n\n

  \n
- High-end machines with substantial computing power are required to solve the puzzle in a timely manner.
  \n
- The electricity required to power the hardware also considerably adds to the cost.
  \n

\n\n

Why is mining attractive yet?

\n\n

  \n
- **Anonymity** - Cryptocurrencies are a boon for individuals or corporations which seek financial anonymity.
  \n
- The lack of a central regulatory authority facilitates trade in illegal goods through the virtual currencies.
  \n
- **Lucrative** - Exchanges that trade bitcoin have witnessed massive hike in prices owing to speculation.
  \n
- The valuation of a single bitcoin was around Rs.65,ooo in January, 2017.
  \n
- Its value had peaked at around Rs.12,60,000 in December 2017.
  \n
- **Hardware assets** - The software for mining cryptocurrencies like bitcoin is open source and available online.
  \n
- But the hardware processing speed required to make mining feasible are found only in high-end workstations that are powered by GPUs.

\n
- Leveraging hardware assets to mine for coins is another means to have a share in the process.
\n

\n\n

What is the latest cryptojacking threat?

\n\n

\n
- A said earlier, cryptocurrency mining is lucrative but still involves huge costs, diminishing the attractiveness.
\n
- To balance the cost overruns, attackers have started employing malware.
\n
- It is a way to force an entry into the computers of remote users, and then using their hardware to mine for coins.
\n
- This is cryptojacking. It is profitable since it eliminates the cost burden of owning a mining assembly with hundreds of processors.
\n

\n\n

Who are vulnerable?

\n\n

\n
- The phenomenon is not restricted to the miniscule minority that trades in cryptocurrencies or uses their systems to mine for coins.
\n
- All users who browse the internet are vulnerable to their systems being ‘cryptojacked’.
\n

\n\n

\n
- Desktops, laptops, tablets, or even mobile devices can be maliciously subverted without the knowledge of their owners.
\n

\n\n

How does crptojacking work?

\n\n

\n
- Cryptojackers usually target popular websites which draw audiences numbering in the millions every day.
\n
- Once the malware patch has been embedded on a website, it infects the web browsers of visitors.
\n
- It slows down their machines, often causing them to overheat.
\n
- Websites and apps that do not charge a fee for consuming their content survive on revenue from digital advertising.
\n
- However, websites like the file-sharing platform have been found to be employing code which hijacks users' system.
\n
- It then uses it for mining cryptocurrency.
\n
- Many websites view this as an alternative source of revenue, bypassing intrusive advertisements.
\n

\n\n

What is the way forward?

\n\n

\n
- The transition to a digital economy has made financial services more dependent on technology.
\n
- The emergence of cryptocurrencies has made it even more difficult to check hackers trying to access online finances.
\n
- It is thus crucial to address the rising concern of cryptojacking.
\n
- There are a range of applications that could protect computers from attacks by cryptojackers.
\n
- Some of them inlcude 'NoCoin', 'MalwareBytes', 'minerBlock'.
\n
- While these tools are not completely infallible, they provide a first line of defence against potential security breaches.
\n

\n\n

\n\n

Source: The Hindu

\n