

What is cryptojacking?

July 29, 2022

In news— According to a report by SonicWall, a US-based cybersecurity firm ‘Cryptojacking’ attacks on computer systems have gone up by 30% in the first half of 2022 compared to the first half of 2021.

Key findings of the report-

- **According to the SonicWall’s Cyber Threat Report,** the crackdown on ransomware attacks is forcing cybercriminals to look for alternative methods. **Cryptojacking involves “lower risk”, and promises “potentially higher payday”.**
- It says that while volume increases were widespread, some business sectors were hit harder than others, such as the finance industry, which saw a rise of 269%.
- Cryptojacking incidents targeting the retail industry rose by 63% year-to-date.
- As per the report, **cryptojacking is an appealing alternative for cybercriminal gangs as it has a lower potential of being detected by the victim;** unsuspecting users across the world see their devices get unaccountably slower, but it’s hard to tie it to criminal activity, much less point to the source.
- **Unlike ransomware, which announces its presence and relies heavily on communication with victims, cryptojacking can succeed without the victim ever being aware of it.**

What is cryptojacking?

- **Cryptojacking is a cyber attack wherein a computing device is hijacked and controlled by the attacker, and its resources are used to illicitly mine**

cryptocurrency.

- In most cases, the **malicious programme is installed when the user clicks on an unsafe link**, or visits an infected website and unknowingly provides access to their Internet-connected device.
- **Coin mining** is a legitimate, competitive process used to release new crypto coins into circulation or to verify new transactions.
- It involves solving complex computational problems to generate blocks of verified transactions that get added to the blockchain. The reward for the first miner who successfully manages to update the crypto ledger through this route is crypto coins.
- **But the race to crack this 64-digit hexadecimal number code needs considerable computing power** involving state-of-the-art hardware, and electrical power to keep the systems involved up and running.
- **Cryptojackers co-opt devices, servers, and cloud infrastructure, and use their resources for mining.** The use of 'stolen' or cryptojacked resources slashes the cost involved in mining.

Why is it a concern?

- **Cryptojacking is hard to detect and the victims of these attacks mostly remain unaware** that their systems have been compromised.
- **Some telltale signs are the device slowing down, heating up**, or the battery getting drained faster than usual.
- **Apart from individuals, businesses too are on the target list of cryptojackers.**
- **The primary impact of cryptojacking is performance-related**, though it can also increase costs for the individuals and businesses affected because coin mining uses high levels of electricity and computing power.