

# Google can detect cryptocurrency mining malware without needing to install software on the user's computer

Because there is no need to install software, detecting cryptocurrency mining malware will not affect the device's performance.

Google has just announced a public beta of its Virtual Machine Threat Detection (VMTD) system. This new system can detect cryptocurrency miners and other malware without needing to install specialized scanning software on users' machines.

Currently, developers and businesses using cloud-based virtual machines are constantly being targeted by hackers. Cyber criminals have found ways to install virtual currency mining tools on victims' virtual machines. This causes the CPU and GPU performance of the virtual machine to be affected, reducing work productivity.



In its 2021 Threat Horizons report, Google said that cryptocurrency mining malware accounts for 86% of all cloud computing virtual machine attacks.

To detect threats on virtual machines, cloud computing service providers often install software running inside the server. This software will act as security software.

However, security software can affect performance, and when a server is compromised, hackers can disable it before deploying malicious code.

Therefore, Google engineers have found a unique approach that does not involve installing security software or remotely collecting data. Google has made changes to its Google Compute Engine hypervisor, the underlying simulation software that virtual machines run inside. The ability to scan and analyze virtual machine memory

and network requests is added so that suspicious activities can be detected.

This approach from Google does not affect performance because there is no need to install additional software.

The VMTD feature is available for trial as early as February 8, 2022 and can be enabled from the Security Command Center. Google also shared an inactive cryptocurrency mining tool on GitHub that admins can use to check if they have correctly configured VMTD on their systems.

Google also guarantees that VMTD will not collect or track any user data.

You finished reading the article "**Google can detect cryptocurrency mining malware without needing to install software on the user's computer**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.