WHAT IS CCLEANER ATTACK?

It was discovered that a malware has been injected into CCleaner, a popular PC optimisation application. It is used by over **75 million users worldwide**. Approximately **2.27 million users were affected** by the malware-laden version.

WHICH VERSIONS WERE AFFECTED?

CCleaner version 5.33.6162 and CCleaner Cloud version 1.07.3191, on 32-bit Windows systems, were illegally modified before they were released to public. .

WHY IS IT DANGEROUS?

A **two-stage backdoor** was injected. This backdoor is **capable of remotely executing code** on the affected systems. It **can be used to spread additional malware, such as ransomware**.

COUNTERMEASURES

1. **Remove the affected versions** of CCleaner and CCleaner Cloud
2. **Download the latest stable release** from Piriform website
3. It is also advised, though not mandatory, to **format and re-install the affected endpoints**
4. Organizations, using an application blacklisting solution, can **block the installation of affected versions** of CCleaner and CCleaner Cloud

This infographic was developed as part of DSCI's Threat Intelligence & Research (Ti&R) Initiative. To know more about or participate in DSCI Ti&R, contact tir@dsci.in

DSCI
PROMOTING DATA PROTECTION
Data Security Council of India