Hundreds of networks were accessed illegally when Codecov was attacked on a large scale

Codecov suffered a relatively small supply-chain attack.

In a new report released by Reuters, investigators claimed that hundreds of networks from various organizations and businesses around the world were compromised in the supply chain attack. target the Codecov platform. This makes the size and nature of the case much more of a concern.

According to a BleepingComputer report last week, Codecov suffered a relatively small supply-chain attack. It is worth mentioning that this offensive campaign has been quietly going on for over 2 months before being discovered. Therefore, the harm it causes is definitely not simple.

During this attack, the threat actors obtained Codecov credentials from the failed Docker images. Hackers then used the images to alter Codecov's Bash Uploader script, which is commonly used by the company's clients.

By replacing Codecov's IP address with his own malicious one in the Bash Uploader script, the attackers found a way to allow them to silently collect client credentials. Codecov - tokens, API keys, and anything that is stored as an environment variable in a client's persistent integration environment (CI) - which is almost undetected.

Codecov is a popular online software testing platform that can be integrated with GitHub projects to generate detailed code reports and statistics. That is why it is particularly popular among more than 29,000 software development businesses worldwide.

Hundreds of customer networks were violated

Codecov's initial investigation shows that as of January 31, 2021, unauthorized changes to the Bash Uploader script have occurred. This gives threat actors the ability to steal Codecov users' information stored in their CI environment.

However, it was not until April 1 that Codecov became fully aware of this malicious activity when a customer noticed the difference between the hash (shashum) of the Bash Uploader script hosted on the Codecov domain and the function. The correct is listed on the company's GitHub.

Soon after, the incident attracted the attention of US federal investigators. The breach has been compared to the recent 'infamous' SolarWinds attacks for which the US government has blamed the Russian Foreign Intelligence Service (SVR).

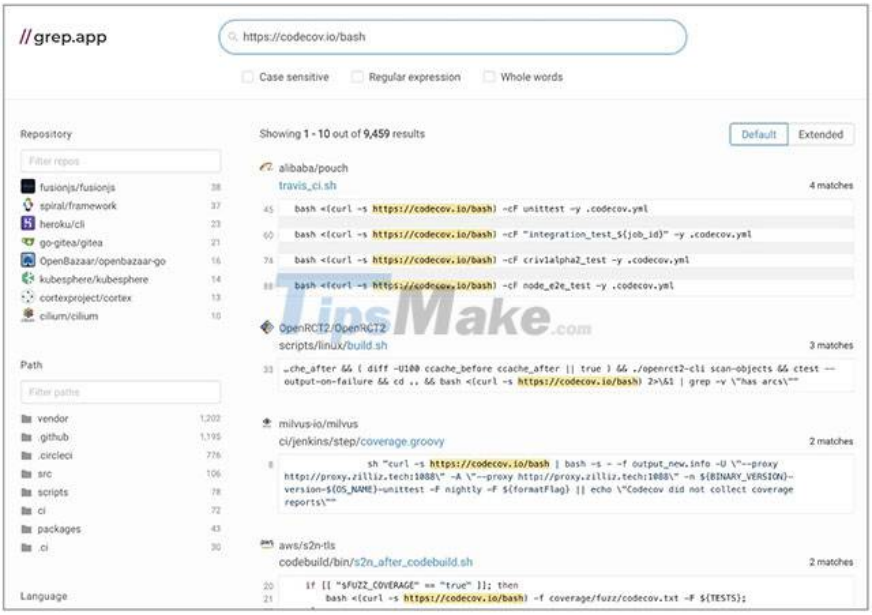
Codecov has more than 29,000 customers worldwide, including prominent names like GoDaddy, Atlassian, The Washington Post, Procter & Gamble (P&G), making this a very concerning supply chain incident.

According to federal investigators, Codecov attackers have deployed automated processes to use the credentials they collect to exploit hundreds of Codecov's customer networks. For this reason, the scope of the breach even went beyond Codecov's systems.

By misusing customer credentials gathered through a Bash Uploader script, hackers were able to obtain the credentials of thousands of other systems, according to the investigator.

Impact investigation

Due to the seriousness and far-reaching scope of the incident, investigators of the US federal government have stepped in and are carefully considering the case.



Several major Codecov customers, including IBM, say their code has not been modified, but declined to comment on whether their systems were breached.

Hewlett Packard Enterprise (HPE), one of the other 29,000 Codecov customers, said it is continuing to investigate the incident:

> "HPE has a dedicated team of experts to investigate this matter, and customers should rest assured, we will give notice of any impact as well as necessary corrective actions as soon as possible. additional information".

The Federal Bureau of Investigation (FBI) and the US Department of Homeland Security (DHS) are not available to comment on the investigation at this time.