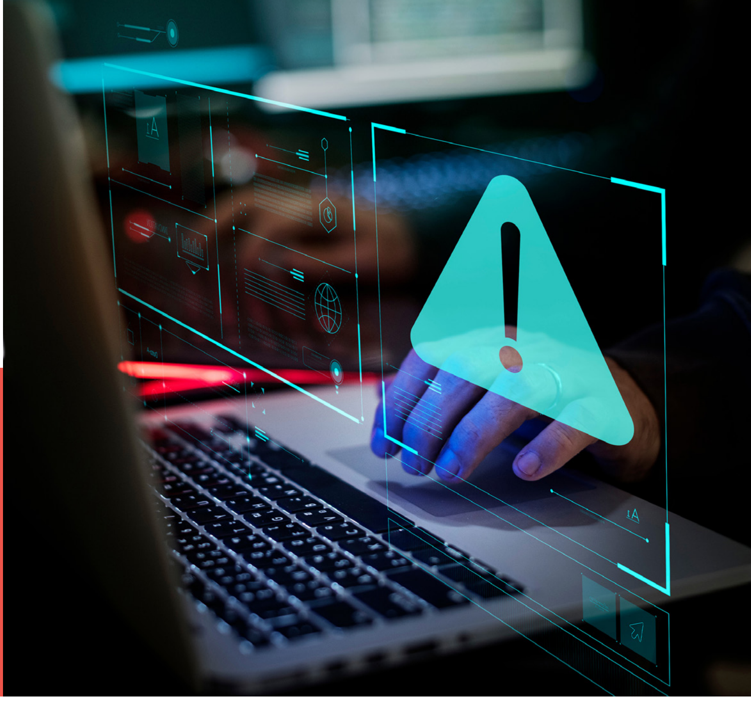
TRACKING THE ACTIVITIES OF TEAMTNT

A Closer Look at a Cloud-Focused Malicious Actor Group



TeamTNT was one of the most prolific malicious actor groups in 2020 and has continued to be so in 2021, launching a number of campaigns aimed primarily at cloud environments. In our comprehensive research on TeamTNT, we take a look at the group's recent activities, specifically the tools, techniques, and payloads it uses in its routines.

KEY FINDINGS

Throughout its campaigns, TeamTNT generally follows the same infection routine. First, the group conducts reconnaissance to search for suitable targets. It then searches for any security weaknesses it could exploit to deliver its payloads.

Credential theft is one of the group's primary objectives. In order to determine its main targets for credential theft, TeamTNT uses its scripts containing functions designed to seek out credentials for specific services and software such as Secure Shell (SSH) and Docker API.

TeamTNT incorporates backdoors and rootkits in its activities. One of the most noteworthy tools in its arsenal is a rootkit called Diamorphine, which it uses to hide the presence of cryptocurrency mining activities via function hooks.

TeamTNT's payloads include credential stealers, cryptocurrency miners, and IRC bots. These payloads have interesting features and functionalities, such as the ability to push out competing malware and the implementation of obfuscation techniques.

Cryptocurrency mining malware such as that used by TeamTNT could result in heavy financial losses for individuals and organizations alike. Aside from potential losses incurred via electricity and internet bills, cryptocurrency mining malware could also cause wear and tear to computers and slow down company operations by using up valuable hardware and software resources.

HOW TO PROTECT CLOUD ENVIRONMENTS FROM ATTACKS

Exploiting cloud misconfigurations and other security weaknesses remains TeamTNT's primary method of compromising cloud environments. To thwart possible attacks by malicious actor groups like TeamTNT, security personnel should follow best practices such as applying the principle of least privilege, implementing stringent authentication measures, and patching software and systems in a timely manner.

Learn more about TeamTNT's activities in our research paper at https://bit.ly/teamtntactivities.

TREND MICRO™ | research