2022 Cloud-Native Threat Report

EXECUTIVE SUMMARY

Cloud Adversary Analysis: TeamTNT

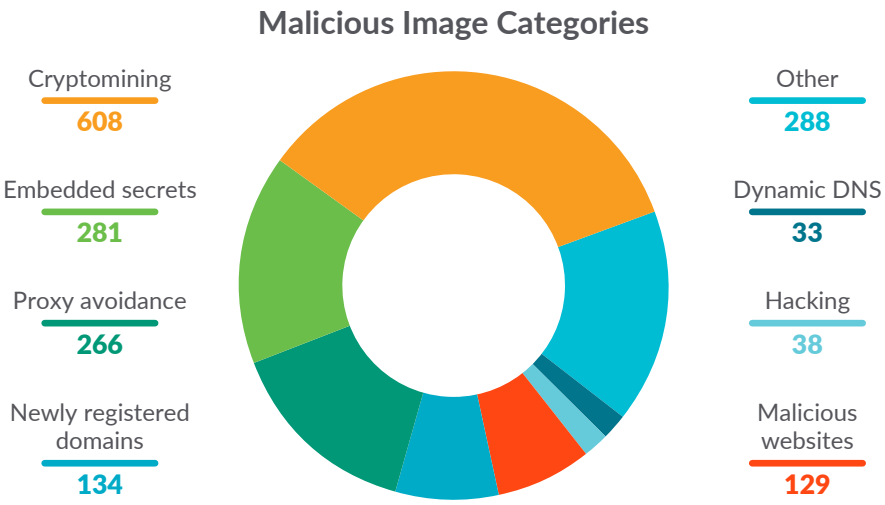
Cryptojacking: low risk, high reward for cloud attackers

TeamTNT is a notorious cloud-targeting threat actor that generates the majority of their criminal profits through cryptojacking. Sysdig TRT attributed more than $8,100 worth of cryptocurrency to TeamTNT, which was mined on stolen cloud infrastructure, costing the victims more than $430,000. The full impact of TeamTNT and similar entities is unknowable, but at $1 of profit for every $53 the victim is billed, the damage to cloud users is extensive.

Supply Chain Attacks Against Containers

Threat actors abuse open ecosystems for evil and profit

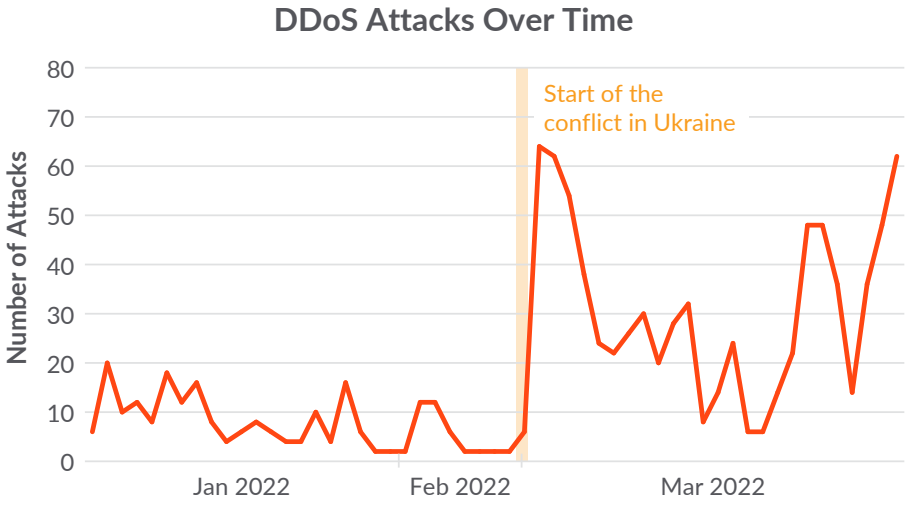
Docker Hub allows for developers of modern applications to easily share container images. Sysdig TRT finds attackers littering the public repository with dangerous container images that contain cryptominers, backdoors, and many other unwelcome surprises, often disguised as legitimate popular software.



Geopolitical Conflict Influences Attacker Behaviors

Cybercriminals take sides, enabled by civilian volunteers

The conflict between Russia and Ukraine includes a cyberwarfare component with government-supported threat actors and civilian hacktivists taking sides. The goals of disrupting IT infrastructure and utilities have led to a four-fold increase in DDoS attacks between 4Q21 and 1Q22. Over 150,000 volunteers have joined anti-Russian DDoS campaigns using container images from Docker Hub. The threat actors hit anyone they perceive as sympathizing with their opponent, and any unsecured infrastructure is targeted for leverage in scaling the attacks.



The Sysdig Threat Research Team (TRT) continuously tracks the emerging threat landscape, focusing on the context of public cloud, containers, Kubernetes, and cloud-native application development. To learn more read our full threat research report.

Learn More

EXEC-SUM-RP Rev. A 9/22