TeamTNT (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 18:19:59 UTC

Since Fall 2019, Team TNT is a well known threat actor which targets *nix based systems and misconfigured Docker container environments. It has constantly evolved its capabilities for its cloud-based cryptojacking operations. They have shifted their focus on compromising Kubernetes Clusters.

2024-09-18 · Group-IB · Nam Le Phuong, Vito Alfano
Storm clouds on the horizon: Resurgence of TeamTNT?
TeamTNT 2023-07-13 · Aqua Nautilus · Assaf Morag, Ofek Itach
TeamTNT Reemerged with New Aggressive Cloud Campaign
TeamTNT 2023-07-05 · Aqua Nautilus · Assaf Morag, Ofek Itach
Threat Alert: Anatomy of Silentbob’s Cloud Attack
TeamTNT Tsunami 2022-07-18 · Palo Alto Networks Unit 42 · Unit 42
Thief Libr
TeamTNT Watchdog 2022-07-18 · Palo Alto Networks Unit 42 · Unit 42
Adept Libra
TeamTNT TeamTNT 2022-03-02 · CyberArk · CyberArk Labs
Conti Group Leaked!
TeamTNT Conti TrickBot 2022-02-18 · Intezer · Intezer
TeamTNT Cryptomining Explosion
TeamTNT 2022-02-09 · vmware · VMWare
Exposing Malware in Linux-Based Multi-Cloud Environments
ACBackdoor BlackMatter DarkSide Erebus HelloKitty Kinsing PLEAD QNAPCrypt RansomEXX REvil Sysrv-hello TeamTNT Vermilion Strike Cobalt Strike 2022-01-01 · Toli Security · Toli Security
Active crypto-mining operation by TeamTNT
TeamTNT 2021-12-07 · sysdig · Alberto Pellitteri
Threat news: TeamTNT stealing credentials using EC2 Instance Metadata
TeamTNT 2021-12-01 · Trend Micro · Trend Micro Research
Analyzing How TeamTNT Used Compromised Docker Hub Accounts
TeamTNT 2021-11-03 · Trend Micro · Alfredo Oliveira, David Fiser
TeamTNT Upgrades Arsenal, Refines Focus on Kubernetes and GPU Environments
TeamTNT 2021-10-07 · Uptycs · Siddharth Sharma
Team TNT Deploys Malicious Docker Image On Docker Hub
TeamTNT 2021-10-06 · Anomali · Tara Gould
Inside TeamTNT’s Impressive Arsenal: A Look Into A TeamTNT Server
TeamTNT 2021-09-14 · Cado Security · Cado Security
TeamTNT Script Employed to Grab AWS Credentials
TeamTNT Tsunami 2021-09-08 · AT&T · Ofer Caspi

TeamTNT with new campaign aka “Chimaera”

TeamTNT 2021-09-01 · Intezer · Intezer

TeamTNT: Cryptomining Explosion

TeamTNT Tsunami 2021-07-20 · Trend Micro · Alfredo Oliveira, David Fiser

Tracking the Activities of TeamTNT: A Closer Look at a Cloud-Focused Malicious Actor Group

TeamTNT 2021-02-20 · Malpedia · Malpedia

Malpedia Website for Malware Family Team TNT

TeamTNT TeamTNT 2021-02-17 · Aquasec · Assaf Morag

Threat Alert: TeamTNT Pwn Campaign Against Docker and K8s Environments

TeamTNT TeamTNT 2021-02-03 · Palo Alto Networks Unit 42 · Ariel Zelivansky, Aviv Sasson, Jay Chen

Hildegard: New TeamTNT Malware Targeting Kubernetes

TeamTNT TeamTNT 2021-01-27 · AT&T · Ofer Caspi

TeamTNT delivers malware with new detection evasion tool

TeamTNT TeamTNT 2021-01-05 · Lacework Labs · Lacework Labs

TeamTNT Builds Botnet from Chinese Cloud Servers

TeamTNT TNTbotinger TeamTNT 2020-12-21 · Intezer · Intezer

Top Linux Cloud Threats of 2020

AgeLocker AnchorDNS Blackrota Cloud Snooper Dacls Doki FritzFrog IPStorm Kaiji Kinsing NOTROBIN Penquin Turla PLEAD Prometei RansomEXX Stantinko TeamTNT TSCookie WellMail elf.wellmess TeamTNT

2020-12-02 · Aqua Nautilus · Assaf Morag, Idan Revivo

Threat Alert: Fileless Malware Executing in Containers

TeamTNT 2020-09-30 · Aqua Nautilus · Assaf Morag

Threat Alert: TeamTNT is Back and Attacking Vulnerable Redis Servers

TeamTNT 2020-08-25 · Aqua Nautilus · Assaf Morag

Deep Analysis of TeamTNT Techniques Using Container Images to Attack

TeamTNT Tsunami XMRIG 2020-08-17 · Cado Security · Chris Doman

Team TNT – The First Crypto-Mining Worm to Steal AWS Credentials

TeamTNT TeamTNT 2020-08-17 · Cado Security · Chris Doman, James Campbell

Team TNT - The First Crypto-Mining Worm to Steal AWS Credentials

TeamTNT

There is no Yara-Signature yet.
