# Commando Cat: A Novel Cryptojacking Attack Abusing Docker Remote API Servers

Date: 7th June 2024 | Severity: High

## Summary

"Commando Cat" is a sophisticated cryptojacking campaign that targets exposed Docker API endpoints. It uses a benign container generated using the Commando Project to infiltrate the system, then executes multiple payloads, including stealing credentials and deploying a cryptocurrency miner. The campaign uses evasion techniques to avoid detection and removal. It's linked to previously observed malware, suggesting the presence of copycat groups. Users and organizations are urged to patch vulnerabilities, secure Docker API endpoints, and implement robust endpoint detection and response (EDR) solutions.

## Attack Vectors

- To gain initial access, the attacker deploys a docker image named cmd.cat/chattr, a harmless docker image. Once deployed, the malicious actor creates a docker container based on this image and uses chroot to break out of the container and gain access to the host operating system. It also uses curl/wget to download the malicious binary into the host.
- The significance of this attack campaign lies in its use of Docker images to deploy cryptojacking scripts on compromised systems. This tactic allows attackers to exploit vulnerabilities in Docker configurations while evading detection by security software. As cybersecurity researchers continue to monitor this malicious actor, it's essential for organizations to strengthen their defenses against Docker-related attacks.

## Indicator of compromise

| INDICATOR TYPE | INDICATORS |
|---|---|
| File Hash | • 9E824EBFCA16F16980172EC0652244C650E48DA3F17EB296BB0A544E68FAA671<br>• 9C7A12678651D72127C3C6E4DAC250439FA4A3BE0A8728754CEA327C86A529A2 |
| URL | • hxxp[:]//leetdbs[.]anondns[.]net/z |
| IPs | • 45[.]9[.]148[.]193<br>• 80[.]239[.]140[.]66<br>• 103[.]127.43.208 |

# Recommendation

- Submit the File Hash to the Antivirus team to update their database with the file hashes.
- Submit the Domains to the Network team to update their database with the Domains.
- Secure RDP ports to prevent threat actors from abusing and leveraging RDP tools.
- Prioritize remediating known exploited vulnerabilities.
- Implement EDR solutions to disrupt threat actor memory allocation techniques.
- Make regular backups of important and critical files.
- Avoid browsing the unsafe websites, clicking on suspicious links, or opening unknown email attachments.
- Update and Patch operating system, applications, and security software's up to date with latest patches.

**NOTE:** The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

# Reference Link

- https://www.trendmicro.com/en_us/research/24/f/commando-cat-a-novel-cryptojacking-attack-.html

Copyright © Mphasis Corporation. All rights reserved