Attackers are rewriting their tools to counter analysis.

Researchers have identified a new malware campaign targeting public APIs (Application Programming Interface), a set of ready-made functions and procedures that allow developers to create software that interacts with other applications or services. An API defines how different software components should interact with each other while ensuring the security and stability of the system. APIs are often used in web development to create sites and applications that use the data and functionality of other services." data-html="true" data-original-title="API" >API Docker is a platform for containerizing applications in the development world The software allows you to package applications with all their dependencies and configuration files into a container that can run on any platform that supports Docker

Docker containers provide isolation of applications from the host operating system and other applications, allowing. create execution environments that can be easily transferred between different hosts and platforms

Using Docker allows you to speed up and simplify the development process, improve the portability and scalability of applications, and also increase the security of their operation. data-html="true" data-original-title="Docker" >Docker for delivering cryptocurrency miners and other malware.

The tools used included a remote access tool capable of downloading and executing additional malware, as well as a utility for distributing malware via SSH, an application-level network protocol that allows remote control of the operating system and tunneling of TCP connections. The protocol is similar in functionality to the Telnet and rlogin protocols, but, unlike them, it encrypts all traffic, including transmitted passwords. SSH allows a choice of different encryption algorithms.

SSH clients and SSH servers are available for most network operating systems.

SSH allows virtually any other network protocol to be transmitted securely in an unsecured environment. Thus, you can not only work remotely on your computer through the command shell, but also transmit an audio stream or video over an encrypted channel." data-html="true" data-original-title="SSH" >SSH, Datadog experts report, is a monitoring and analytics tool that is used to track the performance and health of container environments such as Docker and Kubernetes. It allows you to monitor metrics such as CPU and memory usage, network traffic, and the health of containers. Datadog also integrates with

Kubernetes, making it easy to monitor and manage containers in a Kubernetes environment. To provide secure access to its APIs and data collection, Datadog uses tokens that can be configured for different levels of access, including reading and writing metrics and events. tools for data analysis, creation of dashboards and alerts, which helps operators and developers quickly identify and solve problems in container environments." data-html="true" data-original-title="Datadog" >Datadog in its recent report.

Analysis of the campaign revealed tactical similarities to previous activity known as Spinning YARN, which was identified by Cado Security, a cybersecurity solutions company. It was founded in 2020 and is based in London, UK." data-html="true" data-original-title="Cado Security" >Cado Security and targets misconfigured Apache Hadoop YARN, Docker, Atlassian Confluence and Redis services for Cryptojacking (also called malicious cryptomining) is an online threat that lurks on a computer or mobile device and uses the device's resources to "mine" cryptocurrency. Malicious cryptominers are often installed through a web browser or fraudulent mobile applications. Many types of electronic devices are susceptible to cryptojacking. , including desktop computers, laptops, smartphones and even network servers." data-html="true" data-original-title="Cryptojacking" >cryptojacking.

The attack begins by searching for Docker servers with open ports (port number 2375) and includes several stages: reconnaissance, privilege escalation, and exploitation of vulnerabilities.

Payloads are downloaded using a "vurl" script from attacker-controlled infrastructure. This script includes another script "b.sh" which contains an encoded binary file "vurl". This file, in turn, is responsible for loading and running a third script called "ar.sh" (or "i.sh").

The "b.sh" script decodes and extracts the binary file in "/usr/bin/vurl", overwriting the existing version of the script, as explained by security researcher Matt Muir. "This binary differs from the script version by using hard-coded control domains."

The "ar.sh" script does a variety of things, including creating a working directory, installing tools to scan the internet for vulnerable hosts, disabling the firewall, and loading the next stage of the payload, known as "chkstart".

The main purpose of the Golang binary "vurl" is to configure the host for remote access and load additional tools such as "m.tar" and "top", the latter of which is an XMRig miner – a software for mining the cryptocurrency Monero.
Often used by attackers as a tool for cryptomining without the consent of the computer

owner.” data-html=”true” data-original-title=”XMRig” >XMRig.

In the original Spinning YARN campaign, much of the chkstart functionality was implemented through scripts, Muir explained. Moving this functionality to Go code may indicate an attempt to complicate the analysis process, since static analysis of compiled code is much more complex than analysis of scripts.

Two other payloads are loaded along with “chkstart”: “exeremo” to move to other hosts and spread the infection, and “fkoths” – an ELF binary in Go to hide traces of malicious activity and prevent analysis.

“Exeremo” is also designed to install various scanning tools such as pnscan, masscan and a custom Docker scanner (“sd/httpd”) to detect vulnerable systems.

This update to the Spinning YARN campaign demonstrates a willingness to continue attacks on misconfigured Docker hosts for initial access, Muir noted. Attackers continue to improve their payloads by moving to Go code, which may indicate an attempt to complicate the analysis process or experiment with multi-architecture builds.