Использование контейнера с легитимным названием многократно повысило скрытность преступников.

Исследователи в области кибербезопасности предупредили о новой кампании по криптоджекингу, нацеленной на некорректно настроенные кластеры Kubernetes – открытое ПО для автоматизации развёртывания, масштабирования и координации контейнеризированных приложений в условиях кластера. Поддерживает основные технологии контейнеризации, включая Docker, rkt, а также поддерживает технологию аппаратной виртуализации." data-html="true" data-original-title="Kubernetes" >Kubernetes для майнинга криптовалюты Dero.

Компания Wiz — это стартап, который предоставляет решения для кибербезопасности облачной инфраструктуры AWS, Microsoft Azure и GCP. Компания была основана в 2020 году бывшими руководителями Microsoft Cloud Security Group." data-html="true" data-original-title="Wiz" >Wiz, занимающаяся облачной безопасностью, сообщила, что это обновлённый вариант финансово мотивированной операции, впервые задокументированной CrowdStrike в марте 2023 года.

«В данном инциденте злоумышленник использовал анонимный доступ к кластеру, подключенному к интернету, чтобы запускать вредоносные контейнерные образы, размещённые на Docker Hub, некоторые из которых были загружены более 10 000 раз», — сообщили исследователи Wiz. «Эти образы содержат упакованный с помощью UPX майнер DERO под названием "pause"».

Первичный доступ осуществляется через внешне доступные серверы API (Application Programming Interface) – это набор готовых функций и процедур, которые позволяют разработчикам создавать программное обеспечение, взаимодействующее с другими приложениями или сервисами. API определяет, как различные компоненты программного обеспечения должны взаимодействовать друг с другом, обеспечивая при этом безопасность и стабильность работы системы. API часто используется в веб-разработке для создания сайтов и приложений, которые используют данные и функциональность других сервисов." data-html="true" data-original-title="API" >API Kubernetes с включенной анонимной аутентификацией для доставки полезной нагрузки майнера.

В отличие от версии 2023 года, которая использовала DaemonSet под названием «proxy-api», новая версия использует, на первый взгляд, безобидные DaemonSet под названиями «k8s-device-plugin» и «pytorch-container» для запуска майнера на всех узлах кластера.

Идея названия контейнера «pause» заключается в попытке выдать его за настоящий контейнер «pause», который используется для начальной настройки пода и обеспечения сетевой изоляции.

Майнер криптовалюты представляет собой бинарный файл с открытым исходным кодом, написанный на Go (часто также «Golang») – компилируемый многопоточный язык программирования, разработанный внутри компании Google. Официально язык был представлен в ноябре 2009 года. На данный момент поддержка официального компилятора, разрабатываемого создателями языка, осуществляется для операционных систем FreeBSD, OpenBSD, Linux, macOS, Windows, DragonFly BSD, Plan 9, Solaris, Android, AIX." data-html="true" data-original-title="Go" >Go, который был модифицирован для жёсткого кодирования адреса кошелька и URL-адресов пользовательских пулов майнинга Dero. Он также скрыт с помощью пакера UPX, чтобы усложнить анализ.

Главное преимущество встраивания конфигурации майнинга в код заключается в возможности запуска майнера без каких-либо аргументов командной строки, которые обычно контролируются механизмами безопасности.

Wiz также выявила дополнительные инструменты, разработанные злоумышленником, включая Windows-образец упакованного с помощью UPX майнера Dero, а также скрипт-дроппер, предназначенный для завершения процессов конкурирующих майнеров на заражённом хосте и установки GMiner с GitHub.

«Злоумышленник зарегистрировал домены с невинными названиями, чтобы избежать подозрений и лучше вписаться в легитимный веб-трафик, одновременно маскируя коммуникацию с известными пулами майнинга», — отметили исследователи.

«Эти комбинированные тактики демонстрируют стремление злоумышленника адаптировать свои методы и опережать защитные механизмы».