Злоумышленники переписывают свои инструменты для противодействия анализу.

Исследователи выявили новую кампанию вредоносного ПО, нацеленную на публичные 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 Docker – это платформа для контейнеризации приложений в сфере разработки ПО. Она позволяет упаковывать приложения со всеми их зависимостями и конфигурационными файлами в контейнер, который может быть запущен на любой платформе, поддерживающей Docker.

 Контейнеры Docker обеспечивают изоляцию приложений от операционной системы хоста и других приложений, что позволяет создавать среды исполнения, которые могут быть легко перенесены между различными хостами и платформами.

 Использование Docker позволяет ускорить и упростить процесс разработки, улучшить портируемость и масштабируемость приложений, а также повысить безопасность их работы." data-html="true" data-original-title="Docker" >Docker для доставки криптовалютных майнеров и других вредоносных программ.

В числе используемых инструментов обнаружен инструмент удалённого доступа, способный загружать и исполнять дополнительные вредоносные программы, а также утилита для распространения вредоносного ПО через SSH – сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений. Протокол похож по функциональности с протоколами Telnet и rlogin, но, в отличие от них, шифрует весь трафик, включая и передаваемые пароли. SSH допускает выбор различных алгоритмов шифрования.

 SSH-клиенты и SSH-серверы доступны для большинства сетевых операционных систем.

 SSH позволяет безопасно передавать в незащищённой среде практически любой другой сетевой протокол. Таким образом, можно не только удаленно работать на компьютере через командную оболочку, но и передавать по шифрованному каналу звуковой поток или видео." data-html="true" data-original-title="SSH" >SSH, сообщают эксперты Datadog – это инструмент для мониторинга и аналитики, который используется для отслеживания производительности и состояния контейнерных сред, таких как Docker и Kubernetes. Он позволяет мониторить метрики, такие как использование CPU и памяти, сетевой трафик, а также состояние

контейнеров.

 Datadog также интегрируется с Kubernetes, облегчая мониторинг и управление контейнерами в среде Kubernetes. Для обеспечения безопасного доступа к его API и сбору данных Datadog использует токены, которые можно настроить для различных уровней доступа, включая чтение и запись метрик и событий. Кроме того, Datadog предоставляет инструменты для анализа данных, создания дашбордов и алертов, что помогает операторам и разработчикам быстро выявлять и решать проблемы в контейнерных средах." data-html="true" data-original-title="Datadog" >Datadog в своём недавнем отчёте.

Анализ кампании выявил тактические сходства с предыдущей активностью, известной как Spinning YARN, которая была выявлена компанией Cado Security – это компания, специализирующаяся на предоставлении решений в области кибербезопасности. Она была основана в 2020 году и базируется в Лондоне, Великобритания." data-html="true" data-original-title="Cado Security" >Cado Security и нацелена на некорректно настроенные сервисы Apache Hadoop YARN, Docker, Atlassian Confluence и Redis для Криптоджекинг (также называемый злонамеренным криптомайнингом) — это онлайн-угроза, которая скрывается на компьютере или мобильном устройстве и использует ресурсы устройства для «майнинга» криптовалюты. Вредоносные криптомайнеры часто устанавливаются через веб-браузер или мошеннические мобильные приложения. Криптоджекингу подвержены многие виды электронных устройств, включая настольные компьютеры, ноутбуки, смартфоны и даже сетевые серверы." data-html="true" data-original-title="Криптоджекинг" >криптоджекинга.

Атака начинается с поиска серверов Docker с открытыми портами (номер порта 2375) и включает несколько этапов: разведку, повышение привилегий и эксплуатацию уязвимостей.

Полезные нагрузки загружаются с помощью скрипта «vurl» из инфраструктуры, контролируемой злоумышленниками. Этот скрипт включает в себя другой скрипт «b.sh», который содержит закодированный бинарный файл «vurl». Данный файл, в свою очередь, отвечает за загрузку и запуск третьего скрипта под названием «ar.sh» (или «i.sh»).

Скрипт «b.sh» декодирует и извлекает бинарный файл в «/usr/bin/vurl», перезаписывая существующую версию скрипта, как пояснил исследователь безопасности Мэтт Мьюр. «Этот бинарный файл отличается от версии скрипта использованием жёстко закодированных доменов управления».

Скрипт «ar.sh» выполняет множество действий, включая создание рабочей

директории, установку инструментов для сканирования интернета на наличие уязвимых хостов, отключение брандмауэра и загрузку следующего этапа полезной нагрузки, известной как «chkstart».

Основная цель Golang-бинарного файла «vurl» — настроить хост для удалённого доступа и загрузить дополнительные инструменты, такие как «m.tar» и «top», последний из которых является майнером XMRig – это программное обеспечение для майнинга криптовалюты Monero.
 Зачастую используется злоумышленниками в качестве инструмента для криптомайнинга без согласия владельца компьютера." data-html="true" data-original-title="XMRig" >XMRig.

В оригинальной кампании Spinning YARN большая часть функционала «chkstart» была реализована с помощью скриптов, пояснил Мьюр. Перенос этого функционала на код Go может указывать на попытку усложнить процесс анализа, так как статический анализ скомпилированного кода значительно сложнее, чем анализ скриптов.

Вместе с «chkstart» загружаются две другие полезные нагрузки: «exeremo» для перемещения на другие хосты и распространения инфекции, а также «fkoths» — ELF бинарный файл на Go для сокрытия следов вредоносной активности и противодействия анализу.

«Exeremo» также предназначен для установки различных инструментов сканирования, таких как pnscan, masscan и пользовательский сканер Docker («sd/httpd»), для обнаружения уязвимых систем.

Это обновление кампании Spinning YARN демонстрирует готовность продолжать атаки на некорректно настроенные хосты Docker для первоначального доступа, отметил Мьюр. Злоумышленники продолжают совершенствовать свои полезные нагрузки, переходя на код Go, что может указывать на попытку усложнить процесс анализа или эксперименты с многоархитектурными сборками.