Компания рассказала, как киберпреступники из Китая внедряют виртуальные машины-призраки.

MITRE – некоммерческая организация, основанная в 1958 году, которая управляет исследовательскими центрами, финансируемыми правительством США. Основная цель MITRE – поддерживать ключевые направления государственной политики, обеспечивая техническую поддержку и работу в области исследований и разработок для различных федеральных агентств.

 Одной из наиболее известных инициатив MITRE является база данных общественных уязвимостей, которая предоставляет унифицированный список идентификаторов для уязвимостей в системах безопасности.

 Также стоит отметить, что MITRE разрабатывает и поддерживает множество других инструментов, фреймворков и баз данных, которые активно используются в отрасли кибербезопасности по всему миру." data-html="true" data-original-title="MITRE" >MITRE Corporation сообщила о кибератаке на их некоммерческую организацию в конце декабря 2023 года. Атакующие использовали уязвимости нулевого дня в Ivanti Connect Secure (Industrial Control System (ICS) – это система управления и контроля, которая используется для управления и мониторинга процессов в промышленности. Она обычно включает в себя компьютерные системы, программное обеспечение, сенсоры, контроллеры и другие устройства, которые позволяют автоматизировать и контролировать процессы производства, такие как производство энергии, химические процессы и т.д." data-html="true" data-original-title="ICS" >ICS) для создания поддельных виртуальных машин VMware — поставщик программного обеспечения для виртуализации и облачных вычислений, базирующийся в Пало-Альто, Калифорния. Компания VMware, основанная в 1998 году, является дочерней компанией Dell Technologies. Корпорация EMC первоначально приобрела VMware в 2004 году; Позже EMC была приобретена Dell Technologies в 2016 году. VMware основывает свои технологии виртуализации на своем гипервизоре ESX/ESXi без операционной системы с архитектурой x86." data-html="true" data-original-title="VMware" >VMware.

Злоумышленники получили доступ к серверу vCenter и создали собственные виртуальные машины в среде VMware. Хакеры внедрили веб-оболочку JSP (BEEFLUSH) на сервер vCenter Server Tomcat для запуска инструмента туннелирования на основе Python, что позволило киберпреступникам установить SSH-соединения между созданными виртуальными машинами и инфраструктурой гипервизора ESXi.

Целью атаки было скрыть свои действия от интерфейса централизованного управления (vCenter) и сохранить постоянный доступ, сводя к минимуму риск обнаружения. Подробности атаки появились еще в апреле, когда MITRE установила, что за атакой

стоит китайская группировка UNC5221, которая проникла в исследовательскую среду NERVE (Networked Experimentation, Research, and Virtualization Environment) – интегрированная платформа для проведения сетевых экспериментов и исследований, а также для виртуализации сетевых сред.

 NERVE обеспечивает возможности для моделирования, тестирования и анализа сетевых процессов, создания виртуальных топологий и интеграции с различными инструментами, что позволяет улучшать качество сетевых разработок и исследований в безопасной и контролируемой среде." data-html="true" data-original-title="NERVE" >NERVE с использованием двух уязвимостей ICS (CVE-2023-46805 и CVE-2024-21887).

После обхода многофакторной аутентификации и получения начального доступа, злоумышленники продвинулись по сети, используя скомпрометированную учетную запись администратора для контроля над инфраструктурой VMware. Хакеры развернули несколько бэкдоров и веб-оболочек для сохранения доступа и кражи учетных данных. Среди них был бэкдор на языке Go под кодовым названием BRICKSTORM, а также веб-оболочки BEEFLUSH и BUSHWALK, которые позволяли выполнять произвольные команды и связываться с серверами управления.

Также злоумышленники использовали стандартную учетную запись VMware, VPXUSER, для выполнения семи API-запросов, чтобы перечислить список подключенных и отключенных дисков.

Специалисты объясняют, что поддельные виртуальные машины работают вне стандартных процессов управления и не подчиняются установленным политикам безопасности, что делает их трудно обнаруживаемыми и сложными для управления через графический интерфейс. Для выявления и устранения рисков, связанных с такими машинами, необходимы специальные инструменты или методы.

Одной из эффективных мер противодействия скрытным попыткам атакующих является включение безопасной загрузки, которая предотвращает несанкционированные изменения, проверяя целостность процесса загрузки. Компания также предоставила два скрипта PowerShell [1 и 2] для выявления и устранения потенциальных угроз в среде VMware.

На перекрестке науки и фантазии — наш канал