

Специалисты уже выдвинули предположения, какая хакерская группировка может стоять за распространением вредоноса.

Злоумышленники, стоящие за вредоносным ПО RedTail, добавили недавно обнаруженную уязвимость в брандмауэрах Palo Alto Networks – это международная компания, специализирующаяся на разработке и предоставлении инновационных решений в области кибербезопасности. Компания была основана в 2005 году и с тех пор стала одним из ведущих поставщиков защитных технологий и продуктов.

 Основной продукт Palo Alto Networks – это платформа Next-Generation Firewall (NGFW), которая обеспечивает высокую степень защиты сетей и предотвращает различные киберугрозы. Эти устройства используют интеллектуальные алгоритмы и аналитику для обнаружения и блокировки вредоносного программного обеспечения, включая угрозы на уровне приложений и данных.

 Кроме NGFW, Palo Alto Networks также предлагает другие решения в области кибербезопасности, включая системы обнаружения и предотвращения вторжений (IDS/IPS), системы предотвращения утечек данных (DLP), защиту конечных точек (Endpoint Protection), анализ угроз и безопасность облачных сервисов." data-html="true" data-original-title="Palo Alto Networks" >Palo Alto Networks в свой арсенал атак. В результате обновлений, вредоносное ПО теперь включает новые техники защиты от анализа, что подтверждают эксперты из компании Akamai Technologies, Inc. – поставщик услуг сети доставки контента (CDN), оказывает услуги в сфере кибербезопасности и облачных технологий. Компания была основана в 1998 году и с тех пор стала одним из крупнейших в мире поставщиков CDN, предоставляющим контент и приложения через Интернет для различных отраслей, включая электронную коммерцию, СМИ и развлечения, финансы, здравоохранение и т.д.
 <p> Службы кибербезопасности компании обеспечивают защиту от DDoS-атак, атак на веб-приложения и других угроз, в то время как их облачные сервисы помогают организациям предоставлять свои приложения и сервисы в облаке и управлять ими. Сегодня Akamai располагает глобальной сетью серверов, расположенных в более чем 135 странах, а их клиентами являются некоторые из крупнейших мировых компаний и организаций." data-html="true" data-original-title="Akamai" >Akamai, специализирующейся на веб-инфраструктуре и безопасности.

Специалисты по безопасности Райан Барнетт, Стив Купчик и Максим Заводчик в своём техническом отчёте отметили, что атакующие сделали шаг вперёд, используя частные криптовалютные майнинговые пулы для большего контроля над результатами майнинга, несмотря на возросшие операционные и финансовые затраты.

Атака начинается с использования уязвимости в PAN-OS с идентификатором

CVE-2024-3400, которая позволяет неавторизованному злоумышленнику выполнять произвольный код с правами суперпользователя на Брандмауэр — это устройство сетевой безопасности, которое отслеживает входящий и исходящий сетевой трафик и разрешает или блокирует пакеты данных на основе набора правил безопасности. Его цель — установить барьер между вашей внутренней сетью и входящим трафиком из внешних источников (например, из Интернета), чтобы заблокировать вредоносный трафик." data-html="true" data-original-title="Брандмауэр" >брандмауэре. После успешного взлома, выполняются команды, предназначенные для загрузки и запуска bash-скрипта с внешнего домена, который затем скачивает вредоносное ПО RedTail в зависимости от архитектуры процессора.

RedTail также использует и другие механизмы распространения, эксплуатируя известные уязвимости в маршрутизаторах TP-Link (CVE-2023-1389), ThinkPHP (CVE-2018-20062), Ivanti Connect Secure (CVE-2023-46805 и CVE-2024-21887), а также VMWare Workspace ONE Access и Identity Manager (CVE-2022-22954).

Первое упоминание о RedTail появилось в январе 2024 года, когда исследователь безопасности Патрик Маховяк задокументировал кампанию, использующую уязвимость Log4Shell (CVE-2021-44228) для внедрения вредоносного ПО на системы на базе Unix.

В марте 2024 года компания Barracuda Networks раскрыла детали кибератак, эксплуатирующих уязвимости в SonicWall (CVE-2019-7481) и Visual Tools DVR (CVE-2021-42071) для установки вариантов ботнета Mirai, а также недостатки в ThinkPHP для развёртывания RedTail.

Последняя версия майнера, обнаруженная в апреле, включает значительные обновления, такие как зашифрованная конфигурация, используемая для запуска встроенного майнера XMRig. Также в экземпляре отсутствует жёстко запрограммированный криптовалютный кошелёк, что может свидетельствовать о переходе злоумышленников на частные майнинговые пулы или прокси-пулы.

Эксперты отметили, что последняя конфигурация вредоноса показывает стремление злоумышленников оптимизировать процесс майнинга, в том числе благодаря использованию продвинутых техник уклонения и устойчивости. Всё это свидетельствует о глубоком понимании хакерами принципов работы криптомайнинга.

Akamai охарактеризовала RedTail как высококачественное вредоносное ПО, что редко встречается среди семейств майнеров криптовалют. Точные личности

RedTail: призрачный майнер атакует брандмауэры, скрываясь в криптовалютных пулах

злоумышленников пока неизвестны, однако использование частных майнинговых пулов напоминает тактику, применяемую северокорейской группой Lazarus, которая известна широкомасштабными кибератаками с целью финансовой выгоды.