Хитросплетённая паутина взломов окутала сотни организаций по всему миру.

Исследователи безопасности из компании QiAnXin – это китайская компания, специализирующаяся на кибербезопасности и информационной безопасности. Она предоставляет разнообразные решения и услуги для защиты от киберугроз, включая мониторинг событий, анализ угроз, защиту сетей и данных. Qianxin сотрудничает с различными организациями и предприятиями, помогая им обеспечивать надежную кибербезопасность и предотвращать кибератаки." data-html="true" data-original-title="QiAnXin" >QiAnXin недавно раскрыли долгосрочную кибершпионскую операцию, известную как «APT Operation Veles», направленную против научных и образовательных учреждений по всему миру. Основной подозреваемый — хакерская группа UTG-Q-008, которая специализируется на атаках на Linux-платформы, используя обширную ботнет-сеть.

За год интенсивного мониторинга удалось выявить доказательства использования UTG-Q-008 ресурсов ботнет-сети для кражи данных из научных и образовательных учреждений. Примерно 70% инфраструктуры этой группы составляют промежуточные серверы, которые меняются при каждой новой атаке.

Атаки UTG-Q-008 отличаются высокой интенсивностью и использованием доменов, активных на протяжении последних десяти лет, что делает их более устойчивыми по сравнению с другими известными APT-группами.

UTG-Q-008 использует множество списков атакуемых объектов, один из которых включает более пяти тысяч сетевых сегментов внутри Китая.

Большинство контролируемых узлов находятся в Китае, а сразу за ним следует США. Серверы хакеров часто хранят компоненты для атаки в TAR-формате, используя промежуточные серверы для загрузки и хранения данных. Один из доменов, используемых для атак, зарегистрирован в Китае и действует уже 14 лет.

Для получения доступа к серверам UTG-Q-008 использует компоненты Nanobot, загружаемые через wget или Curl с промежуточных серверов. Эти компоненты позволяют хакерам запускать обратные shell-сессии или SSH-туннели для загрузки дополнительных модулей.

UTG-Q-008 применяет различные типы внутренних сканеров для проверки открытых портов в сетях. После завершения сканирования они передают результаты для дальнейшего перемещения по сети.

Процесс перемещения включает два этапа: сканирование SSH-портов на серверах и использование слабых паролей для доступа. Хакеры используют специальную базу паролей, включающую более 4000 учётных данных, собранных за годы атак.

При необходимости входа в сеть, атакующие используют FRP обратные прокси-серверы, которые позволяют использовать внешние вычислительные мощности ботнет-сети для взлома важных внутренних серверов.

Достигнув значительного уровня проникновения, UTG-Q-008 устанавливает на ключевых серверах модули для кражи данных. Эти модули анализируют различные файлы и журналы системы, извлекая из них конфиденциальную информацию.

На серверах с мощными графическими картами, хакеры устанавливают компоненты для майнинга криптовалют, что помогает скрыть их основные цели и затруднить расследование.

За последние три года было зафиксировано более 1500 пострадавших IP-адресов, среди которых образовательные сети Китая (CER) занимают значительную долю. Среди пострадавших также есть зарубежные университеты, исследовательские институты и компании в сфере информационных технологий.