Кибершпионы проникли в сердце мировой дипломатии.

Кибершпионская группа SneakyChef нацелилась на МИДы и посольства как минимум 9 стран по всему миру. Специалисты В компании Cisco, которая занимается разработкой и продажей сетевого оборудования, есть подразделение Talos. Оно занимается исследованиями в области угроз информационной безопасности." data-html="true" data-original-title="Cisco Talos" >Cisco Talos предполагают, что за атаками стоят хакеры из Китая, которые собирают информацию о различных геополитических напряженностях в разных частях планеты.

SneakyChef использует в качестве приманки поддельные правительственные документы. Обнаруженная кампания отличается более широким спектром целей, затрагивая страны в Европе, на Ближнем Востоке, в Африке и Азии, тогда как ранее злоумышленники в основном нацеливались на Южную Корею и Узбекистан.

География жертв SneakyChef

Злоумышленники использовали метод передачи зараженных файлов через SFX-архивы RAR, которые при запуске разархивируются и запускают вредоносный VB-скрипт, сохраняющий вредоносное ПО в системе жертвы.

В основе операций SneakyChef лежит инструмент удаленного доступа SugarGh0st, впервые представленный Talos в ноябре прошлого года. Инструмент является модифицированной версией известного Gh0st RAT, который используется различными группами с 2008 года, и впервые был замечен в операциях, связанных с Китаем.

Новый отчет Talos также включает анализ нового трояна удаленного доступа под названием SpiceRAT, который доставляется целям SneakyChef с того же электронного адреса. Такие находки подчеркивают масштабную и интенсивную деятельность хакеров, направленную на разработку кибершпионского ПО против ключевых геополитических объектов.

Цепочка заражения SneakyChef

Пока что SneakyChef отслеживается как отдельная кампания или подразделение, и нет достаточных доказательств, чтобы связать их с какой-либо конкретной государственной структурой или известной группировкой. Однако в майском отчете Palo Alto Networks Unit 42 некоторые связанные активности были классифицированы

как работа китайской APT-группы, что обычно подразумевает активную поддержку правительства.

На перекрестке науки и фантазии — наш канал