Масштабная разведоперация затронула 75 организаций на острове.

С ноября 2023 по апрель 2024 года исследователями безопасности Insikt Group – это подразделение компании Recorded Future, специализирующееся на исследовании угроз в области кибербезопасности. Группа занимается анализом и мониторингом киберактивностей, выявлением и изучением киберугроз, а также разработкой стратегий для защиты от них. В своих расследованиях группа использует разнообразные источники данных, предоставляя доклады и аналитические материалы, которые помогают организациям и государственным учреждениям защититься от сложных и развивающихся киберугроз." data-html="true" data-original-title="Insikt Group" >Insikt Group была зафиксирована кибершпионская кампания, направленная на государственные, академические, технологические и дипломатические организации Тайваня. По данным специалистов, за этими атаками стоит кибергруппа RedJuliett, предположительно связанная с Китаем и действующая из города Фучжоу. Эту группу также называют Flax Typhoon и Ethereal Panda.

Помимо Тайваня, RedJuliett атакует организации в Джибути, Гонконге, Кении, Лаосе, Малайзии, на Филиппинах, в Руанде, Южной Корее и США. В общей сложности, наблюдалось взаимодействие с инфраструктурой этой группы у 24 организаций, включая государственные учреждения Тайваня, Лаоса, Кении и Руанды. Около 75 тайваньских организаций стали объектами более широкой разведки и последующей эксплуатации.

Как сообщается, RedJuliett использует устройства с доступом к Интернету, такие как фаерволы, балансировщики нагрузки и VPN-продукты, для начального доступа. Группа также применяет SQL-инъекции и уязвимости обхода каталогов против веб- и SQL-приложений.

RedJuliett, как ранее сообщалось CrowdStrike и Microsoft, использует программное обеспечение SoftEther для туннелирования вредоносного трафика из сетей жертв и LotL-техники для маскировки. Группа активно действует с середины 2021 года.

Эксперты также отметили, что RedJuliett использует SoftEther для управления операционной инфраструктурой, включающей серверы, арендованные у поставщиков VPS, и скомпрометированную инфраструктуру трёх тайваньских университетов. После успешного начального доступа группа использует веб-оболочку China Chopper для поддержания присутствия, а также другие веб-оболочки с открытым исходным кодом, такие как devilzShell, AntSword и Godzilla. В некоторых случаях была использована уязвимость повышения привилегий в Linux под названием Dirty Cow (CVE-2016-5195).

RedJuliett, вероятно, интересуется сбором информации об экономической политике Тайваня, а также его торговых и дипломатических отношениях с другими странами. Как и многие другие китайские кибергруппы, RedJuliett атакует уязвимые устройства с доступом в Интернет, поскольку они имеют ограниченную видимость и слабые решения безопасности, что делает их эффективными для начального доступа.

Министерство иностранных дел Китая отвергло обвинения, назвав их «сфабрикованной дезинформацией». Тем не менее, эксперты по кибербезопасности продолжают фиксировать активность RedJuliett и подобных ей групп. Международное сообщество выражает растущую обеспокоенность масштабами и изощрённостью кибершпионских кампаний, призывая к усилению глобального сотрудничества в сфере цифровой безопасности.