Длительная кампания показала, как проводится кибершпионаж на государственном уровне.

Специалисты Sophos – компания, которая занимается разработкой и производством средств защиты информации для настольных компьютеров, серверов, почтовых систем и сетевых шлюзов. Разработчики Sophos создают программные и аппаратные продукты для фильтрации спама, борьбы с вирусами и шпионским ПО. Помимо этого, компания также разрабатывает криптографические средства и DLP-системы." data-html="true" data-original-title="Sophos" >Sophos выявили сложную и долгосрочную кибершпионскую операцию китайских госхакеров, направленную на поддержание постоянного доступа к сети правительственной организации в Юго-Восточной Азии. Кампания получила название Crimson Palace.

Кибершпионы стремились получить доступ к критически важным ИТ-системам, проводить разведку конкретных пользователей, собирать конфиденциальную военную и техническую информацию, а также разворачивать различные вредоносные программы для удалённого управления.

Хотя имя целевой правительственной организации не было раскрыто, известно, что страна, в которой она находится, имеет постоянные территориальные конфликты с Китаем в Южно-Китайском море. Это позволяет предположить, что речь может идти о Филиппинах, которые ранее уже подвергались атакам китайской группы Mustang Panda.

Операция Crimson Palace включает 3 кластера активности, некоторые из которых используют одинаковые тактики:

По данным Sophos, являются частью скоординированной кампании, организованной одной группировкой с большим набором инструментов, разнообразной инфраструктурой и несколькими операторами.

Пересечение Кластера Alpha с другими субъектами угроз

Кампания примечательна использованием неизвестных ранее вредоносных программ, таких как PocoProxy, а также обновленной версии EAGERBEE и других известных семейств вредоносных программ, включая NUPAKAGE, PowHeartBeat, RUDEBIRD, DOWNTOWN (PhantomNet) и EtherealGh0st (также известный как CCoreDoor).

Также характерными чертами кампании стали обширное использование техники DLL Sideloading и необычные методы скрытности. Злоумышленники использовали множество новых методов обхода защиты:

Различия и совпадения трех кластеров

В отчете Sophos также приводятся индикаторы компрометации (IoC) для каждого кластера активности, а пока специалисты продолжают расследовать кампанию, чтобы выяснить дополнительные подробности об атаках. Отметим, что HUI Loader ранее использовался китайскими группировками в атаках на игорный сектор Юго-Восточной Азии с целью шпионажа.