Методы группы подозрительно похожи на другие известные угрозы.

Индонезийские государственные службы подверглись масштабной кибератаке со стороны группировки Brain Cipher. 20 июня 2024 года хакеры нанесли серьезный удар по критически важной инфраструктуре страны, парализовав работу около 210 национальных и местных правительственных сервисов. Особенно сильно пострадали таможенные и иммиграционные службы, что привело к существенным задержкам для путешественников в аэропортах.

Изначально злоумышленники потребовали выкуп в размере 8 миллионов долларов США. Однако позже они неожиданно опубликовали дешифратор бесплатно. Этот случай привлек внимание специалистов из компании Group-IB , которые решили провести тщательное расследование деятельности группировки.

Хакеры оставляли на зараженных системах характерные записки с требованием выкупа. В них содержались инструкции по связи с группировкой для расшифровки данных. Контактная информация варьировалась от адресов электронной почты до ссылок на скрытые сервисы в сети Tor.

Исследователи установили, что Brain Cipher активна как минимум с апреля 2024 года. Анализ различных вариантов записок с требованием выкупа позволил связать эту группу с другими хакерскими объединениями, такими как EstateRansomware и SenSayQ.

Одним из ключевых открытий стала связь записок Brain Cipher с образцами вредоносного ПО Lockbit. Эксперты также обнаружили сходство в стиле и содержании уведомлений с теми, что использовала группировка SenSayQ. Более того, онлайн-инфраструктура обеих групп, включая сайты в сети Tor, использовала схожие технологии и скрипты.

Интересно, что контактные адреса электронной почты групп SenSayQ, EstateRansomware и еще одной неназванной группировки совпадали. Первые следы деятельности EstateRansomware были обнаружены в апреле 2024 года. На основании этих данных исследователи предположили, что за Brain Cipher и EstateRansomware могут стоять одни и те же лица.

Brain Cipher не ограничились атакой на Индонезию. Жертвы их нападок были обнаружены также на Филиппинах, в Португалии, Израиле, ЮАР и Таиланде. У группы есть собственный сайт утечек данных (DLS), на котором на момент написания статьи

были опубликованы данные семи компаний.

Большинство уведомлений с требованием выкупа, оставленных Brain Cipher, были связаны с образцами вредоносного ПО, определяемого как Lockbit. Кроме того, группа опубликовала дешифратор на Linux для индонезийской жертвы, который оказался вариантом образца программы-вымогателя Babuk.

Анализ показал, что в июле 2024 года атаки с похожими записками проводились уже под именем группы RebornRansomware. Жертвы этой группы были обнаружены во Франции, Китае, Кувейте и Индонезии.

Интересны и особенности работы сайта утечек данных Brain Cipher. На нем размещалась информация о взломанных компаниях, причем для каждой утечки был установлен таймер обратного отсчета. Такая тактика создавала дополнительное давление на жертв и вынуждала их быстрее принимать решение о выплате.

Аналитики Group-IB — один из ведущих разработчиков решений для детектирования и предотвращения кибератак, выявления мошенничества, исследования высокотехнологичных преступлений и защиты интеллектуальной собственности в сети." data-html="true" data-original-title="Group-IB" >Group-IB составили хронологию событий, показывающую изменения в записках с требованием выкупа предположительно связанных групп программ-вымогателей. Некоторые жертвы Brain Cipher были обнаружены даже в августе 2024 года, а часть жертв SenSayQ была добавлена на их сайт утечек позже в июне 2024 года.

Сходство в записках, корреляция адресов электронной почты и хронологическая последовательность смены названий позволяют предположить, что за EstateRansomware, SenSayQ, Brain Cipher и RebornRansomware стоят одни и те же лица. Однако исследователи воздерживаются от предположений о причинах постоянной смены бренда группы в эпоху активной охоты на крупные программы-вымогатели.

Group-IB отмечает, что их команда продолжит следить за деятельностью Brain Cipher, независимо от того, какое новое имя эта группа может выбрать в будущем. Эксперты подчеркивают важность постоянного мониторинга и анализа деятельности подобных группировок для разработки эффективных методов защиты от их атак.

В заключение Group-IB дали ряд рекомендаций по защите от подобных атак. Среди них: регулярный мониторинг и аудит учетных записей, внедрение политики

управления обновлениями, сегментация критически важных систем, внедрение контроля приложений на хостах и решений для обнаружения и реагирования на конечных точках (EDR). Также рекомендуют подписаться на услугу управляемого поиска угроз (MTH).