Начальная цена «эксклюзивных данных» – 5 биткоинов.

Крупное американское издание The Washington Times стало новой жертвой программы-вымогателя Rhysida. В среду хакерская группировка разместила информацию об атаке на своем сайте в даркнете, заявив о намерении продать «эксклюзивные данные» газеты на онлайн-аукционе.

Злоумышленники установили семидневный срок до начала торгов, призывая потенциальных покупателей «подготовить кошельки». Стартовая цена за предполагаемый массив данных составляет 5 биткоинов, что эквивалентно 292 030 долларам США по курсу криптовалют на четверг.

The Washington Times, базирующаяся в Вашингтоне ежедневная газета правого толка, считается одним из десяти наиболее посещаемых консервативных медиа-ресурсов в США. По данным Statista , ежемесячно сайт издания привлекает более 3 миллионов посетителей, а ежедневный тираж печатной версии превышает 50 000 экземпляров.

Газета была основана во время администрации Рейгана как альтернатива более либеральной The Washington Post. Группировка Rhysida не уточнила объем якобы похищенных с серверов Times данных, но предоставила образец в качестве «доказательства» атаки.

Несмотря на то, что образец трудно разобрать, специалисты Cybernews смогли его изучить. По их словам, он содержит различные корпоративные файлы, включая банковские выписки, документы сотрудников, а также копию водительских прав штата Техас и карточки социального страхования некоего лица.

На момент публикации новости сайт The Washington Times работал без видимых сбоев. Издание было открыто в 1982 году международным медиаконгломератом News World Communications, связанным с христианским религиозным движением «Церковь объединения».

Помимо The Washington Times, «Церковь объединения», последователей которой прозвали «мунитами» по имени ее корейского основателя и лидера Сан Мён Муна, владеет несколькими другими медиа-ресурсами по всему миру. Среди них американское информационное агентство United Press International (UPI), а также газеты в Японии, Южной Корее и Южной Америке.

Группировка Rhysida с момента появления в мае 2023 года заявила о 114 жертвах на

своем сайте в даркнете. По данным обновленного профиля Министерства обороны США, банда проникла в различные секторы, включая образование, здравоохранение, производство и местные органы власти.

Rhysida работает по модели «вымогательское ПО как услуга» (Программа-вымогатель как услуга (Ransomware-as-a-Service, RaaS) – это бизнес-модель, при которой программа-вымогатель сдается в аренду киберпреступникам.

 Разработчик вымогательского ПО предоставляет готовый код шифровальщика другим хакерам. Клиент арендует код шифровальщика у его автора, настраивает его под себя, а затем использует в атаках по своему усмотрению.

 В Raas-модели разработчик программы-вымогателя забирает себе небольшой процент от выкупа жертвы, а большая часть средств достается атакующему.
" data-html="true" data-original-title="RaaS" >RaaS), продавая свои хакерские инструменты коллегам-преступникам за долю прибыли. Хакеры часто практикуют двойное вымогательство: даже после того, как жертва заплатила за ключ дешифрования , они угрожают опубликовать украденные данные, если не получат вторую выплату.

В этом году группировка взяла на себя ответственность за взлом национальной Британской библиотеки, считающейся крупнейшим в мире хранилищем исторических знаний, а также детской больницы Anne & Robert H. Lurie в Чикаго. После того, как требование о выкупе в размере 4 миллионов долларов (60 BTC) не было выполнено, Rhysida опубликовала все документы клиники.

В 2023 году жертвами атак стали калифорнийский медицинский конгломерат Prospect Medical Holdings (PMH), что привело к сбоям в работе десятков больниц и медицинских учреждений в нескольких штатах, а также мюнхенская компания по производству видеоигр Travian Games.

В феврале этого года исследовательская группа из Корейского агентства по безопасности в интернете (KISA) смогла взломать код шифрования банды и опубликовала на своем сайте бесплатный инструмент дешифрования Rhysida, а также руководство по его использованию. Это значительный шаг в борьбе с деятельностью группировки, который может помочь будущим жертвам восстановить свои данные без необходимости платить выкуп.