Злоумышленники зашифровали данные как минимум 210 местных служб.

Министерство связи Индонезии объявило, что хакеры зашифровали системы в национальном центре обработки данных страны с помощью программы-вымогателя. В результате атаки произошли сбои в работе иммиграционных проверок в аэропортах и других общественных услуг

Системы Временного национального центра обработки данных (Temporary National Data Center, PDNS) были заражены Brain Cipher, новым вариантом пресловутой программы-вымогателя LockBit 3.0. Атака затронула филиал PDNS, расположенный в Сурабае. Взлом может привести к утечке данных госучреждений и местных органов власти.

В Министерстве связи сообщили, что злоумышленники потребовали выкуп в размере $8 миллионов в обмен на расшифровку данных. Подчеркивается, что правительство не будет выполнять требования вымогателей.

Кибератака началась 20 июня и затронула такие службы, как оформление виз и вид на жительство, паспортные услуги и системы управления иммиграционными документами. Из-за атаки в аэропортах образовались длинные очереди на иммиграционных стойках. К 24 июня большинство затронутых иммиграционных услуг были восстановлены, а важные данные перенесены в облако.

Атака также затронула платформу, используемую для онлайн-зачисления в школы и университеты, что вынудило правительство региона продлить срок регистрации. В общей сложности программа-вымогатель нарушила работу как минимум 210 местных служб.

По предварительным данным, атака началась с отключения функции безопасности Защитника Windows 17 июня в 23:15 по местному времени, что позволило вредоносной активности продолжаться. Действия начались 20 июня в 00:54. Они включали в себя установку вредоносных файлов, удаление важных файлов и отключение работающих сервисов. Были отключены и выведены из строя файлы, связанные с хранением данных, такие как VSS, HyperV Volume, VirtualDisk и Veaam vPower NFS. Защитник Windows перестал функционировать 20 июня 2024 года в 00:55, что усугубило ситуацию.

Хотя расследование атаки все еще продолжается, власти страны изолировали зараженные сети. Возможности анализа атаки ограничены, так как системы были

зашифрованы. Министерство связи отказалось комментировать инцидент. Пробы вымогательского ПО будут анализироваться с привлечением сторонних ИБ-компаний для предотвращения подобных инцидентов в будущем.

Хотя хакеры использовали программу-вымогатель LockBit, вполне возможно, что за взломом стоит другая группа. Известно, что ряд злоумышленников используют утекший в сеть сборщик LockBit 3.0 и заявляют, что он принадлежит им. Например операторы SEXi использовали билдер и недавно атаковали центр обработки данных в Чили.

Аналитик по кибербезопасности Доминик Альвиери заявил изданию Recorded Future News, что LockBit пока не добавила правительство Индонезии на свой сайт утечек. Обычно внесение в список задерживается из-за переговоров. Так как организации в Индии и Индонезии известны тем, что они не платят вымогателям, в данном случае, вероятно, ситуация повторяется.