настоящее время

РАССЛЕДОВАНИЯ

"Система": работающие против Запада российские хакеры атаковали мэрию Чебаркуля. Они требовали выкуп – но у города не оказалось денег

Настоящее Время Расследовательский проект "Система"

12 июня 2025 года 10:21 мск

LockBit – одна из самых активных хакерских группировок в мире. Она атакует компании, больницы и госучреждения по всему миру, требуя выкуп за расшифровку данных. По версии американских властей и журналиста Брайана Кребса, группой вымогателей может руководить 32-летний Дмитрий Хорошев из Воронежа, ранее использовавший псевдоним putinkrab.

Ранее считалось, что LockBit не трогает российские цели. "Система" убедилась, что это не так.

"В ГУ нервничают"

В мае 2025 года в сеть утекла внутренняя база данных LockBit – архив переписок с жертвами. Утечка охватывает период с декабря 2024-го по апрель 2025-го. В ней 208 уникальных "клиентов" – то есть жертв, с которыми велись переговоры. Из них минимум три общались по-русски и, вероятно, находятся в России. Один из "клиентов" прямо назвал себя:

Я администратор в горуправлении Чебаркуля. Уже больше 24 часов стараемся систему и вэб-сайт восстоновить. Не получилось. Ничего не работает и пока восстонавления нету.

СМОТРИТЕ ТАКЖЕ:
Великобритания обвинила хакеров ГРУ во взломе около 10 тыс. камер на границе Украины и стран Европы для слежки за поставками западной помощи

Чебаркуль – небольшой город в Челябинской области. 24 апреля 2025 года, когда была совершена атака, на официальном сайте мэрии Чебаркуля появилась заставка LockBit с требованием выкупа, обнаружила "Система" в архиве интернета. Средняя сумма выкупа LockBit составляет $19 тысяч, подсчитали в нидерландской компании Defenced.

– *привет, выдам декриптор [расшифровщик данных]. Много залочить успели?* – спросил оператор LockBit у администратора из Чебаркуля.

– *Бесплатно ли это? Горуправление не может выплатить за декриптор, мало денег*, – ответил чебаркулец.

– *конечно бесплатно, это проделки конкурентов наших.*

При этом оператор LockBit не стал отрицать, что при шифровании данных использовался вирус самой LockBit (иначе бы он не предлагал свой расшифровщик).

СМОТРИТЕ ТАКЖЕ:

Белорусские "Киберпартизаны": Роскомнадзор в мае запустит в соцсетях ботов, которые будут собирать данные для российских спецслужб

Расшифровщик, впрочем, не сработал. *"Старались на разных компах, и хотя ПО исполняется, файлы оно не декриптит. <...> Обнаруживает зашифрованные файлы, но не декриптит их. Чтож делать?"* – сетовал сотрудник мэрии. Затем он отправил еще два сообщения – *"Куда пропал? Нужна помощь! В ГУ [горуправлении] нервничают"* и *"Чтоб исправиться, то ГУ обратится к федеральным властям".*

Оператор-вымогатель попытался дать чебаркульцу технический совет, но тот перестал отвечать. Сайт мэрии города не работает до сих пор.

За информацию, которая приведет к аресту Хорошева, власти США предлагают $10 млн. Россия, как правило, не выдает обвиняемых в киберпреступлениях за границу.

В LockBit и мэрии Чебаркуля не ответили на вопросы "Системы".

При участии Рийн Альяс

СМОТРИТЕ ТАКЖЕ:

- Кэш и политический трэш. Фонды, близкие к Дмитрию Медведеву, получили рекордные пожертвования во время войны – мы узнали, на что их тратят
- "Система": родственник Путина недолго руководил компанией с миллиардными господрядами. Теперь ему грозит штраф за искажение отчетности
- Дон Данон. Как люди Кадырова заполучили российские заводы Danone и управляют ими
- Российский теневой флот перекачивает нефть недалеко от петербургских пляжей – под угрозой экология всего Финского залива
- Принудительное трудоустройство "ветеранов": компании в нескольких регионах России обяжут брать на работу участников войны в Украине
- Налет дронов на Москву и Подмосковье: в Дубне под удар попал завод беспилотников "Кронштадт", в Зеленограде – технопарк "Элма"

МАТЕРИАЛ ИЗ РАЗДЕЛОВ:

Новости | Россия | Актуальное | Расследования