Новая группа вымогателей Shadow атакует крупные промышленные предприятия России / Хабр

habr.com/ru/companies/f_a_c_c_t/news/730034/

EditorF_A_C_C_T

EditorF_A_C_C_T 19 апр в 12:00

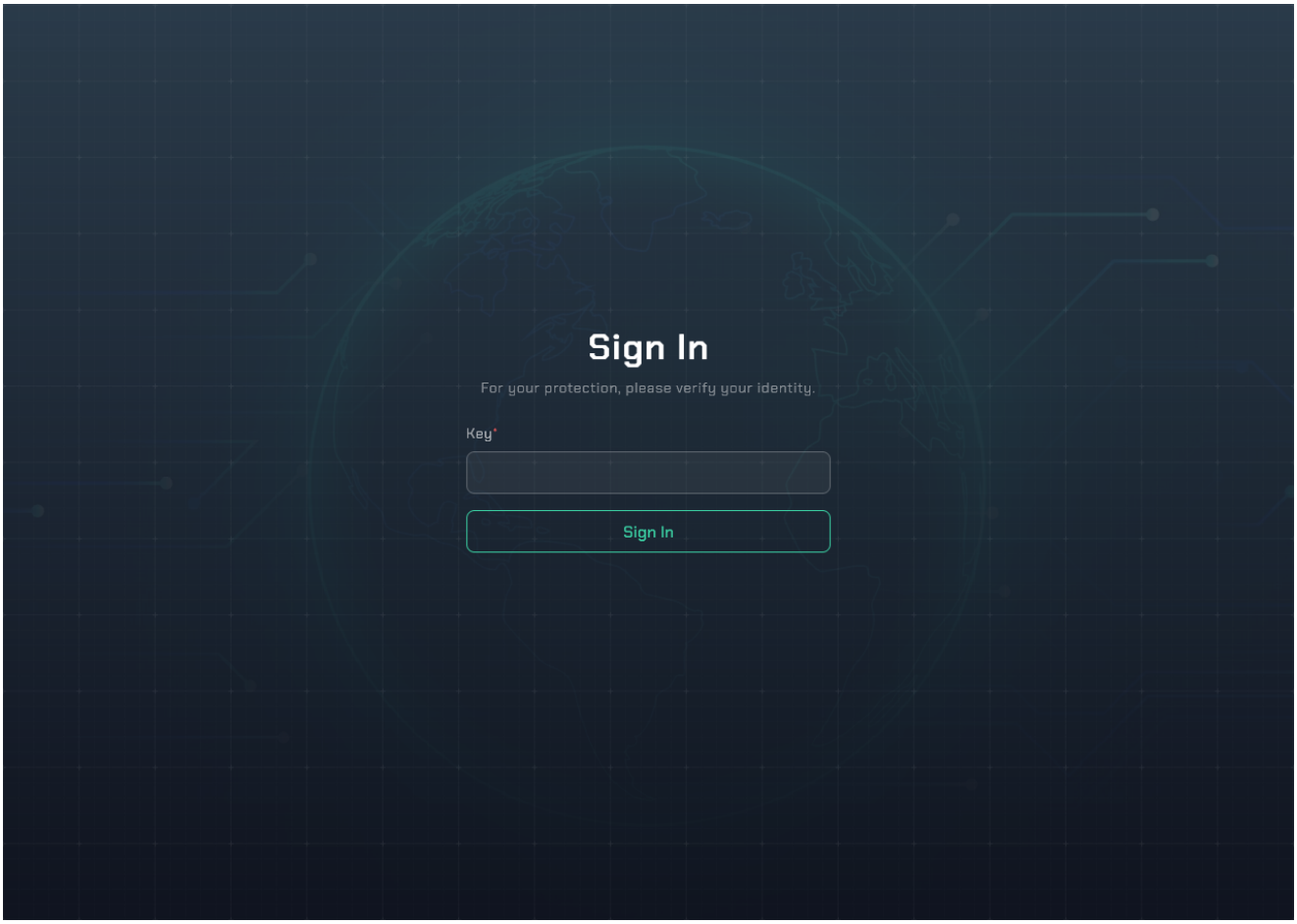
Новая группа вымогателей Shadow атакует крупные промышленные предприятия России

2 мин

1.4K

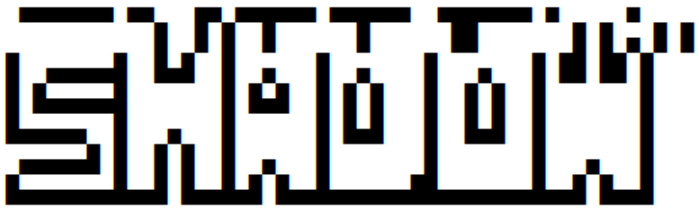
Блог компании F.A.C.C.T. Информационная безопасность *

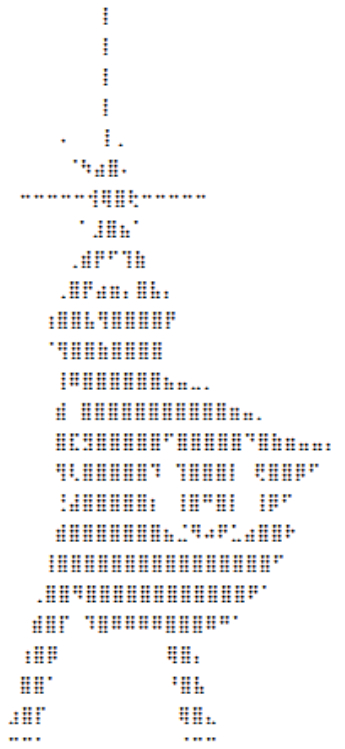
Эксперты Лаборатории компьютерной криминалистики Group-IB зафиксировали атаки новой группы вымогателей Shadow на крупные российские компании. Группа активна, как минимум, с середины марта этого года. За расшифровку данных злоумышленники требуют от жертвы сумму от $1-2 млн. Для общения с каждой жертвой злоумышленники размещают в сети Tor панель с чатом, доступ в которую представитель атакованной компании получает при помощи персонального ключа из записки с требованием выкупа. Такая же система взаимодействия с жертвами используется в известных партнерских программах RaaS (Ransomware-as-a-Service).



Так выглядит вход на панель жертвы

Если компания откажется платить выкуп, представители Shadow угрожают опубликовать данные в даркнете (см записку от Shadow). Отметим, что ранее вымогатели практически не использовали в России подобный инструмент шантажа, ограничиваясь угрозами не предоставить ключ для расшифровки данных. Публикация скаченных данных жертв на DLS-сайтах характерна для атак вымогателей на компании из США, Европы, Азии. В качестве гарантий того, что преступники исполнят свои обещания, представители Shadow уверяют, что они не являются «политически мотивированными и их не интересует что-то еще, кроме денег».





~~~ Your files was encrypted by Shadow Ransomware~~~
>>>> Your data are stolen and encrypted

The data will be published on TOR website if you do not pay the ransom
Link for Tor Browser:

>>>> What guarantees that we will not deceive you?
We are not a politically motivated group and we do not need anything other than your money.
If you pay, we will provide you the programs for decryption and we will delete your data.
Life is too short to be sad. Be not sad, money, it is only paper.

If we do not give you decrypters, or we do not delete your data after payment, then nobody will pay us in the future.
Therefore to us our reputation is very important. We attack the companies worldwide and there is no dissatisfied victim after payment.

>>>> You need contact us and decrypt one file for free on these TOR sites with your personal DECRYPTION ID

Download and install TOR Browser https://www.torproject.org/
Write to a chat and wait for the answer, we will always answer you.
Sometimes you will need to wait for our answer because we attack many companies.

Записка, которую получают жертвы вымогателей
~~~

Как выяснили криминалисты Group-IB, злоумышленники проникают в инфраструктуру жертв через уязвимые публичные сервисы, в т.ч. RDP-серверы. Данные компаний Shadow шифруют с помощью версии популярной программы-вымогателя LockBit3, собранного на основе появившегося в публичном пространстве исходного кода. Для Linux используется шифровальщик на основе исходных кодов вымогателя Babuk. В ходе расследования инцидента специалистами Group-IB выявлен факт ошибочного набора атакующими команды PowerShell на украинской раскладке клавиатуры. Кроме того, выявлены инструменты, аналогичные использованным в атаках неизвестной группировкой на российские банки в 2018 году.

Напомним, что по данным исследования Group-IB, в 2022 году количество кибератак финансово-мотивированных хакеров увеличилось почти в три раза по сравнению с 2021 годом. Самым популярным типом киберугроз, с которыми столкнулись во время реагирований эксперты Лаборатории компьютерной криминалистики Group-IB стали атаки с использованием программ-вымогателей — на них пришлось 68% всех инцидентов. Наиболее агрессивными группами программ-вымогателей в России в прошлом году стали Phobos, CryLock и Sojusz, а рекорд по сумме требуемого выкупа поставила группа OldGremlin, потребовав от жертвы 1 млрд рублей.