Статья Pay2Key - Краски сгущаются

Введение

На прошлых выходных мы сообщили о волне атак с использованием невиданного ранее штамма, получившего название "Pay2Key". Наше расследование показало, что операторы программ-вымогателей в основном нацелены на израильские компании. Программа-вымогатель, использованная в атаках, быстро распространилась по сетям жертв, оставляя значительные части сети зашифрованными вместе с запиской о выкупе, что угрожает утечкой украденных корпоративных данных, если выкуп не будет выплачен.

По мере того, как накапливается все больше и больше сообщений об атаках Pay2Key, мы стали видеть, как жертвы платят выкуп, потому что они не хотели рисковать, обнаружив, что их конфиденциальные корпоративные данные публикуются в Интернете. Однако эта неприятная ситуация также дала возможность понять, кто стоит за этим новым вымогателем.

В этой последующей статье мы поделимся некоторыми из наших новых выводов, а также тем, как мы отслеживали транзакции биткойнов от записок злоумышленников с выкупом до иранской биржи биткойнов. Это стало возможным благодаря совместным усилиям с Whitestream - аналитической фирмой по блокчейн-технологиям.

More Sightings

Вскоре после того, как мы опубликовали первоначальный анализ, мы получили дополнительную информацию из различных источников, проливающую свет на эту новую и загадочную кампанию. Сбор информации показал, что лица, стоящие за Pay2Key, уделяют особое внимание израильским компаниям, хотя в новом отчете Swascan говорится, что по крайней мере одна жертва стала мишенью в Европе.

Двойное вымогательство

Двойное вымогательство, недавнее развитие в сфере программ-вымогателей, о которых мы сообщали в последнее время, представляет собой тактику, которая оказывает дополнительное давление на жертв, чтобы они заплатили выкуп, угрожая утечкой корпоративных данных, украденных из сетей жертв в Интернете.

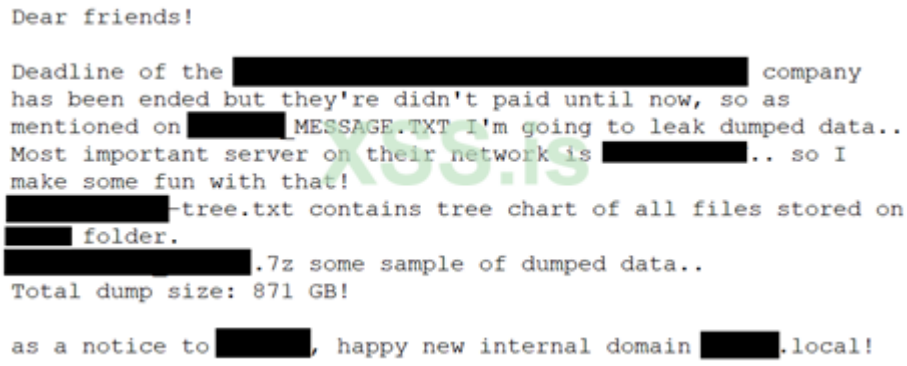
Как сообщалось в нашем первоначальном анализе, операторы Pay2Key следуют этой тенденции - угрожая жертвам посредством записки с требованием выкупа, которую они оставили, для утечки "важной информации ... в случае, если мы не сможем заключить выгодную сделку!"

```
Congratulations!
Your entire network and all your informations such as computers/ employees information/ users folders/ servers/ file-servers/
Some of your important information dumped and ready to leak, in case we can't make a good deal!

Don't modify encrypted files or you can damage them and decryption will be impossible!
Don't try unofficial decryptors to recover your files or you can damage them and decryption will be impossible!
```

Похоже, что авторы Pay2Key готовы оправдать свои угрозы, поскольку они запустили новый веб-сайт Onion, посвященный утечке данных, украденных у не платящих жертв Pay2Key.

На данный момент неуплачиваемыми жертвами этого нападения с двойным вымогательством являются три израильские компании, и к моменту публикации этого отчета их может быть больше. Утечка данных каждой компании-жертвы была загружена в специальную папку на веб-сайте вместе с индивидуальным сообщением от злоумышленников. В сообщении они делятся конфиденциальной информацией о цифровых активах жертвы, включая подробности об их домене, серверах и резервных копиях.



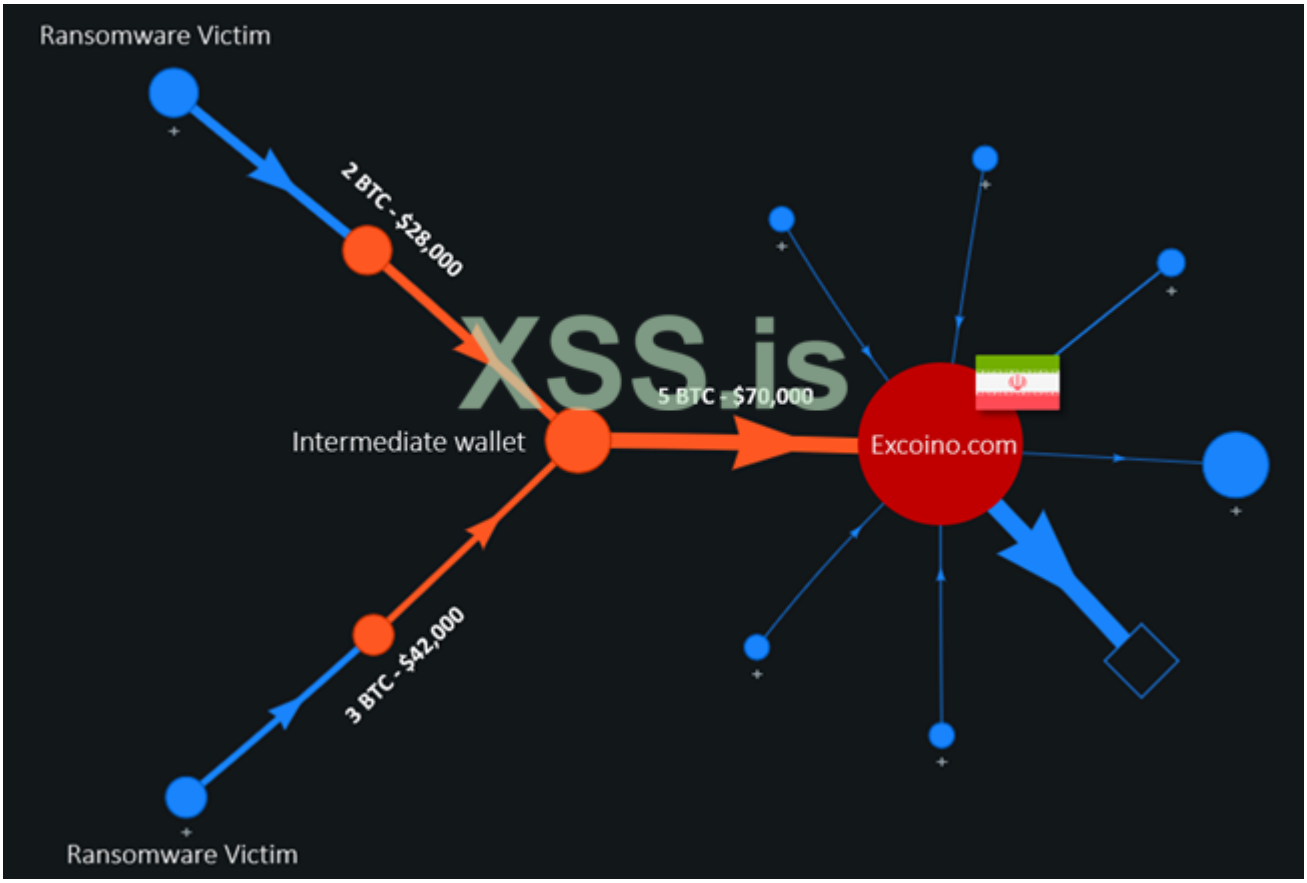
Чтобы лучше понять метод вымогательства, мы делимся тактикой, которую хакер использовал в этой кампании двойного вымогательства - одну против компании по разработке игр, а другую - против юридической фирмы.

В то время как в случае с юридической фирмой много конфиденциальной информации сразу же просочилось по истечении крайнего срока, в случае компании-разработчика игр злоумышленники предложили второй шанс произвести платеж и начали с публикации только подробной древовидной схемы файловой системы NAS-серверы жертвы. Однако через день они уже показади данныеиз папки "Финансы", призывая жертву заплатить до того, как просочится какая-либо дополнительная информация. В обоих случаях злоумышленники указали, что у них были украдены сотни гигабайт данных.

Следуя за деньгами

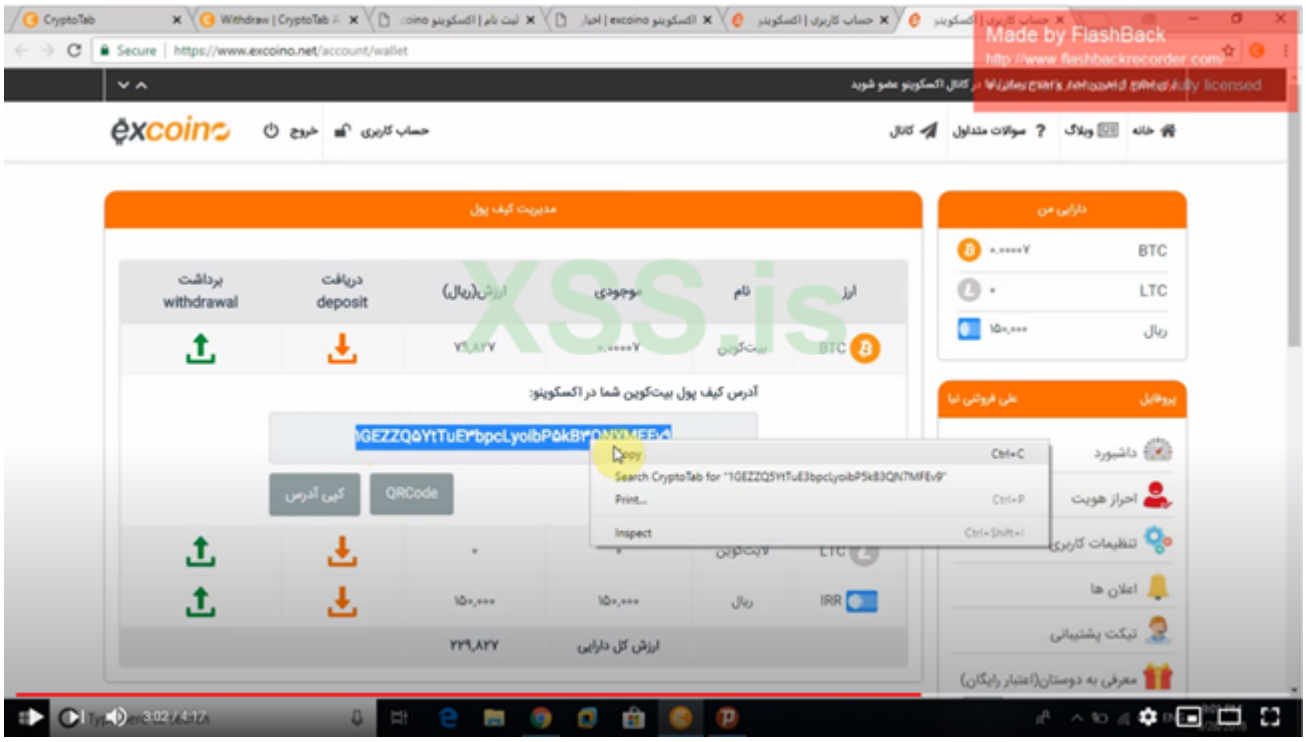
Хотя вышеупомянутые жертвы решили не платить выкуп, было по крайней мере четыре жертвы, которые предпочли заплатить. Эти неудачные обстоятельства создали возможность следить за деньгами и понять, кто может стоять за целевой атакой программы-вымогателя Pay2Key.

Вместе с Whitestream мы отслеживали последовательность транзакций, которые начинались с внесения выкупа и заканчивались тем, что выглядело как иранская биржа криптовалют под названием Excoino.

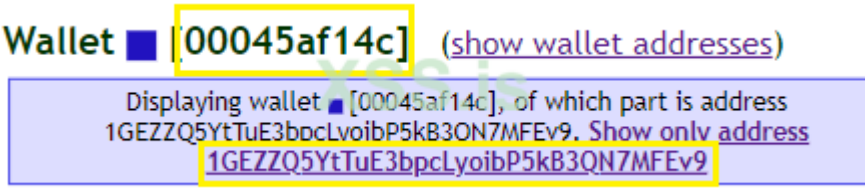


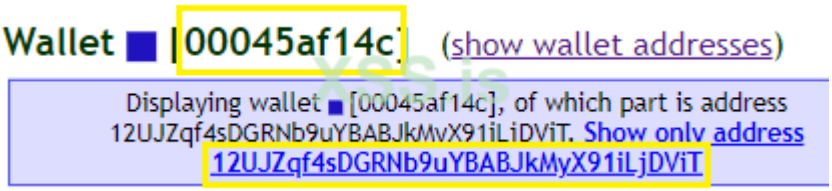
Процесс начинается с биткойн-кошельков, найденных в записках с требованием выкупа. После того, как жертва вносит средства в кошелек для выкупа, указанный в записке о выкупе, злоумышленники переводят деньги в промежуточный кошелек - этот кошелек, как было замечено, повторно использовался для выплаты выкупа несколькими жертвами. Затем биткойн переводится на последний адрес кошелька, связанный с кластером высокой активности. Эти типы кластеров с высокой активностью часто предполагают связь с финансовой организацией, связанной с рынком биткойнов, часто с биржей.

Чтобы проверить связь между этим "последним кошельком" и биржей Excoino, мы использовали службу WalletExplorer и известный адрес кошелька Excoino.



Анализируя адрес биткойна, показанный на рисунке 7, а также наш "последний кошелек", мы видим, что они оба имеют один и тот же идентификатор кластера [00045af14c] согласно WalletExplorer.





Excoino - иранская компания, которая предоставляет услуги безопасных транзакций криптовалюты для граждан Ирана. Регистрация требует, чтобы у пользователя был действующий иранский номер телефона и ID/код Melli (کد ملی). Однако, чтобы иметь право торговать на бирже, также потребуется копия самого идентификатора.

В своих условиях Excoino заявляет, что о первой транзакции (и любой другой подозрительной транзакции) необходимо сообщить в иранскую киберполицию, FATA, для дальнейшего расследования.

Это может означать, что владельцами последних кошельков являются граждане Ирана, которые, скорее всего, стоят за атакой Pay2Key на израильские компании на прошлой неделе.

Заключение

Операторы Pay2Key перешли к стадии двойного вымогательства в ходе своей атаки, утечки данных некоторых из своих "клиентов", пытаясь заставить их (и других) заплатить.

Чтобы отследить действия злоумышленника, стоящего за Pay2Key, мы решили сосредоточиться на кошельках криптовалюты, обнаруженных в записках о выкупе, отслеживая денежный поток на иранскую биржу.

Это, вместе с тем фактом, что атаки, по всей видимости, нацелены на израильские организации, укрепляет наше предположение о том, что эта волна атак действительно совершается иранским лицом, создающим угрозу.

Pay2Key - это лишь последняя волна в серии целевых атак с использованием программ-вымогателей, развернутых в Иране против израильских организаций в течение последних месяцев, и эта тенденция, по всей видимости, набирает обороты.

Источник: https://research.checkpoint.com/2020/pay2key-the-plot-thickens/
Автор перевода: yashechka
Переведено специально для https://xss.is