«Сайты позора» и обратный отсчёт: как киберпреступники давят на жертв.

Все чаще люди, отправляясь по обычным повседневным делам – в школу, больницу или аптеку, сталкиваются с неработающими компьютерными системами. За этими инцидентами нередко стоят преступные группировки из разных уголков планеты, блокирующие системы и требующие выкуп за восстановление доступа или возврат похищенных данных.

Эпидемия программ-вымогателей не показывает признаков замедления в 2024 году, несмотря на усилия правоохранительных органов, и эксперты опасаются, что вскоре она может перейти в более жестокую фазу. «Мы определенно проигрываем борьбу с шифровальщиками сейчас», — говорит аналитик по угрозам компании Recorded Future – это американская компания, которая использует искусственный интеллект и машинное обучение для сбора и анализа информации из открытых источников, таких как новости, социальные сети, блоги, форумы и т.д. Она предоставляет своим клиентам инструменты для принятия решений на основе анализа больших объемов данных, что позволяет им предсказывать события, риски и тренды в различных областях, включая кибербезопасность, финансы, государственную безопасность и т.д." data-html="true" data-original-title="Recorded Future" >Recorded Future Аллан Лиска.

Программы-вымогатели могут стать определяющим киберпреступлением последнего десятилетия, атакуя широкий круг жертв, включая больницы, школы и правительства. Злоумышленники шифруют критически важные данные, останавливая работу жертвы, а затем вымогают деньги, угрожая обнародованием конфиденциальной информации. Эти атаки имеют серьёзные последствия. В 2021 году компания Colonial Pipeline стала жертвой атаки программ-вымогателей, что вынудило её приостановить поставки топлива и заставило президента США Джо Байдена принять экстренные меры для удовлетворения спроса. Однако атаки программ-вымогателей происходят ежедневно по всему миру – на прошлой неделе они нанесли удар по больницам в Великобритании. Многие из них даже не попадают в заголовки новостей.

«Существует проблема с прозрачностью – большинство организаций не раскрывают и не сообщают о подобных инцидентах», – отмечает аналитик по угрозам компании Emsisoft – это компания, специализирующаяся на разработке программного обеспечения в сфере кибербезопасности. Она предоставляет решения для защиты от вредоносных программ, включая антивирусы, антишпионские программы и брандмауэры. Кроме того, Emsisoft также предлагает услуги дешифрования файлов, которые были затронуты программами-вымогателями." data-html="true" data-original-title="Emsisoft" >Emsisoft Бретт Кэллоу. По его словам, это затрудняет оценку

динамики роста атак-вымогателей. Исследователям приходится полагаться на данные госучреждений, подвергшихся атакам, или самих преступников.

Судя по всему, проблема не только не исчезнет, но и обострится в 2024 году. Согласно отчету Mandiant , хакеры все чаще прибегают к публикации похищенных данных на так называемых «сайтах позора». В 2023 году количество публикаций на таких ресурсах выросло на 75% по сравнению с 2022 годом. Эти сайты используют броские тактики, такие как обратный отсчёт до момента, когда конфиденциальные данные жертв будут обнародованы, если они не заплатят.

«Их тактики становятся всё более жестокими», — говорит Кэллоу.

Например, хакеры начали напрямую угрожать жертвам устрашающими телефонными звонками или электронными письмами. В 2023 году Онкологический центр Фреда Хатчинсона в Сиэтле подвергся атаке-вымогателя, в результате которой пациентам с онкологическими заболеваниями рассылались электронные письма с угрозами обнародовать их личную информацию в случае отказа от оплаты.

«Меня беспокоит, что это очень скоро может перейти в реальное насилие», – опасается Кэллоу. «Если речь идет о миллионах долларов, они могут причинить вред руководителю компании, которая отказывается платить, или членам его семьи».

Хотя пока не было зарегистрировано случаев насилия в результате атак-вымогателей, хакерские группировки уже используют подобные угрозы в своей тактике. «В ходе переговоров, которые просочились в сеть, они намекали на подобные действия, заявляя: "Мы знаем, где живет ваш генеральный директор"», – рассказывает Лиска.

Говоря о бесчувственном подходе преступников к жизни и смерти, стоит отметить, что, по оценкам исследователей, с 2016 по 2021 годы атаки программ-вымогателей привели к смерти от 42 до 67 пациентов Medicare из-за задержек с оказанием жизненно важной помощи.

Аналитики также обеспокоены связями между группировками, специализирующимися на атаках-вымогателях, и «The Comm» – неформальной международной сетью преступников, которые предлагают услуги по противоправным действиям онлайн, помимо традиционных киберпреступлений, такими как подмена SIM-карты. Участник Comm рекламируют свою готовность применять физическую силу, повреждать имущество и выкладывать видео, якобы изображающие акты жестокого обращения

В последнее время правоохранительные органы добились некоторых успехов в пресечении деятельности группировок, занимающихся атаками-вымогателями. Например, в феврале международная операция «Cronos» ликвидировала известную хакерскую группу LockBit, конфисковав их веб-сайты и предложив жертвам бесплатную расшифровку данных.>

Трудность в снижении объёмов атак программ-вымогателей отчасти заключается в том, что банды вымогателей — которые работают почти как стартапы, иногда предлагая услугу подписки и круглосуточную поддержку своего программного обеспечения, одновременно привлекая участников для проведения атак — часто базируются в странах, недоступных для высылки. Это побудило западные правоохранительные органы использовать тактики запугивания и психологические игры самих банд против них.

Например, операция «Кронос» использовала таймер обратного отсчёта в стиле сайта позора, чтобы раскрыть личность предполагаемого босса LockBit, 31-летнего гражданина Дмитрия Хорощёва . Ему также предъявили обвинения по 26 пунктам, выдвинутым американскими прокурорами, и наложили санкции. Хотя его арест в стране пребывания маловероятен, раскрытие личности может подорвать доверие к нему и сделать его мишенью.

«Найдутся люди, готовые применить силу, чтобы доставить его через границу в страну, откуда его можно будет экстрадировать». Сообщники также могут беспокоиться о возможности его ареста, если он добровольно покинет страну своего пребывания.

Ещё одной преградой на пути к контролю над программами-вымогателями является гидра-образная природа участников. После нейтрализации LockBit аналитики заметили, что почти сразу появилось 10 новых сайтов, распространяющих шифровальщики. «Это беспрецедентное число за месяц», – констатирует Лиска.

Но правоохранители адаптируются и к этом. В мае международная операция под названием «Endgame» объявила, что ей удалось прервать работу нескольких групп, распространяющих вредоносное ПО, известное как «дропперы». Дропперы являются важной частью экосистемы киберпреступлений, так как позволяют хакерам незаметно доставлять программы-вымогатели или другой вредоносный код. Операция «Endgame» привела к аресту четырёх человек в Армении и Украине, закрытию более 100 серверов и захвату тысяч доменов. «Endgame» использовала психологические тактики, подобные операции «Кронос», такие как обратный отсчёт до видеороликов с текстом, призывающих преступников «подумать о следующем шаге».

Несмотря на масштабы проблемы, Лиска и Кэллоу не теряют оптимизма. Кэллоу полагает, что запрет на выплату выкупа хакерам стал бы самым эффективным решением. Лиска менее уверен в перспективах запрета, но отмечает, что действия правоохранительных органов могут со временем привести к реальным результатам.

«Мы часто говорим о "игре в крота", когда речь идёт о группах вымогателей — одну уничтожишь, появляется другая», — говорит Лиска. «Но я думаю, что [правоохранительные] операции постепенно сужают поле. В конечном итоге, надеюсь, их будет появляться всё меньше и меньше».