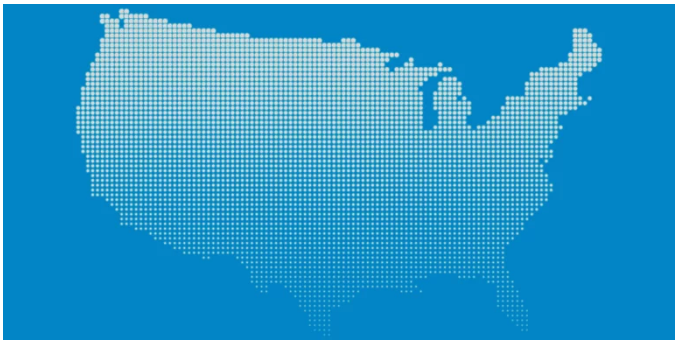
КОММЕНТАРИИ · ЛАБОРАТОРИЯ ВРЕДОНОСНЫХ ПРОГРАММ · ПРОГРАММЫ-ВЫМОГАТЕЛИ · В ЦЕНТРЕ ВНИМАНИЯ ПРОГРАММЫ-ВЫМОГАТЕЛИ

Состояние программ-вымогателей в США: отчет и статистика за 2023 год

ЛАБОРАТОРИЯ ВРЕДОНОСНЫХ ПРОГРАММ EMSISOFT · 2 ЯНВАРЯ 2024 Г. · 12 МИНУТ ЧТЕНИЯ



> ***“По нашим оценкам, с 2016 по 2021 год от атак программ—вымогателей погибло от 42 до 67 пациентов программы Medicare”. - Макглэйв, Непраш и Никпай; Школа общественного здравоохранения Университета Миннесоты***[1]

В 2023 году США вновь подверглись шквалу финансово мотивированных атак программ-вымогателей, которые лишили американцев доступа к критически важным сервисам, скомпрометировали их личную информацию и, вероятно, убили некоторых из них.

В общей сложности 2207 больниц, школ и органов государственной власти США подверглись прямому воздействию программ-вымогателей в течение года, причем многие другие пострадали косвенно в результате атак на их цепочки поставок. Кроме того, это прямо или косвенно затронуло тысячи компаний частного сектора.

Мы считаем, что единственное решение кризиса с программами–вымогателями, который является самым серьезным, каким он когда–либо был, - это полный запрет выплаты выкупов. Мы обсудим, почему мы считаем это действие необходимым, в следующем разделе.

В таблице ниже показано количество организаций, на которые были оказаны воздействия за каждый из последних трех лет.

	2021	2022	2023
Больничные системы*	27	25	46
K-12 школьных округов*	62	45	108
Высшие учебные заведения	26	44	72
Правительства	77	106	95

Итоги	**192**	**220**	**321**

** Скомпрометированы больничные системы нескольких больниц и школьные округа нескольких школ. Общее количество пострадавших больниц и школ описано в разделах по секторам ниже.*

Обратите внимание, что собрать статистическую информацию об инцидентах с программами-вымогателями далеко не просто, поскольку сообщается или разглашается лишь незначительная часть инцидентов. Кроме того, даже при раскрытии инцидентов организации нередко используют запутывающий язык – например, называют инциденты “событиями шифрования”, а не “атаками программ–вымогателей”, - что затрудняет отслеживание на основе поиска. Хотя в этом отчете собраны данные из нескольких источников, неизбежно, что некоторые инциденты не будут учтены, и, следовательно, масштабы проблемы почти наверняка занижены.

Почему следует запретить выплаты выкупа

Как уже отмечалось, программы-вымогатели, по оценкам, убивали примерно одного американца в месяц в период с 2016 по 2021 год, и, вероятно, это продолжается. Чем дольше проблема с программами-вымогателями остается нерешенной, тем больше людей погибнет от них. И, конечно же, экономический ущерб и множество социальных проблем, наносимых программами-вымогателями, также будут продолжаться до тех пор, пока проблема не будет устранена.

Правительства сформировали целевые группы, международные коалиции и обязались на федеральном уровне не выплачивать выкупы,[2] в то время как правоохранительные органы нарушили работу всей экосистемы программ-вымогателей, демонтировали ботнеты, изъяли криптоактивы и произвели аресты. Но, несмотря на все это, программы-вымогатели упорно остаются такой же серьезной проблемой, как и прежде.

Единственный действенный механизм, с помощью которого правительства могут быстро сократить объемы программ-вымогателей, - это запретить выплаты выкупов. Программы-вымогатели - это прибыльное предприятие. Если оно станет нерентабельным, большинство атак быстро прекратятся. Вот что сказал исследователь в области безопасности Кевин Бомонт.[3]

> *“Я серьезно — платежи программ-вымогателей этим группам должны быть объявлены вне закона на международном уровне. Мы должны преодолеть кратковременную боль, потому что это более безопасный вариант. Начните планировать это, громко сигнализируйте об этом и делайте это. Для этого требуется твердое руководство с самого верха, поскольку лоббирование против этого будет реальным. Гражданское общество нуждается в защите посредством твердого руководства, а не руководства небольшого числа фирм, извлекающих выгоду из статус-кво. Это шанс для мировых лидеров руководить, когда другие этого не сделали. ”*

Он прав. Запрет действительно является более безопасным вариантом. Мы можем либо прекратить выплаты выкупа сейчас и остановить программы-вымогатели немедленно, либо мы можем продолжать нести человеческие и финансовые издержки, пытаясь выработать альтернативные стратегии.

Аллан Лиска, аналитик по анализу угроз в Recorded Future, согласен с этим.

> *“Я годами сопротивлялся идее полного запрета на выплаты выкупов, но я думаю, что это должно измениться. Количество программ-вымогателей становится все хуже, причем не только из-за количества атак, но и из-за агрессивного характера атак и групп, стоящих за ними. То, что мы делаем, просто не работает. Да, правоохранительные органы стали лучше, но правоохранительные органы не могут действовать достаточно быстро и бессильны против непокорных государств, таких как Россия, которые отказываются сотрудничать. Запрет на выплаты выкупов будет болезненным и, если верить истории, скорее всего, приведет к кратковременному увеличению числа атак программ-вымогателей, но, похоже, на данный момент это единственное решение, которое имеет шансы на долгосрочный успех. Это прискорбно, но такова реальность, с которой мы сталкиваемся.”*

Бретт Кэллоу, аналитик угроз в Emsisoft, также является сторонником запрета.

> *“Текущие стратегии борьбы с программами-вымогателями сводятся к созданию лежачих полицейских и избиению кротов. Реальность такова, что мы не собираемся защищать наш выход из этой ситуации, и мы также не собираемся контролировать наш выход из нее. До тех пор, пока платежи с помощью программ-вымогателей остаются законными, киберпреступники будут делать все возможное для их получения. Единственное решение - финансово сдерживать атаки, полностью запретив выплату требований. На данный момент запрет - это единственный подход, который, вероятно, сработает.*

До сих пор правительства избегали введения запретов, вероятно, из–за потенциального воздействия на жертв - последствий, которые Целевая группа по программному обеспечению-вымогателю затронула в отчете за 2021 год.[4]

> *“Сложность заключается в определении того, как реализовать такую меру на практике, поскольку по-прежнему отсутствует уровень организационной кибербезопасности в разных секторах, размерах организаций и географических регионах. Злоумышленникам, использующим программы-вымогатели, не требуется большого риска или усилий для запуска атак, поэтому запрет на выплаты выкупа не обязательно приведет к их перемещению в другие области. Скорее всего, они продолжат организовывать атаки и проверять решимость как организаций-жертв, так и их регулирующих органов. Чтобы оказать дополнительное давление, они будут нацелены на организации, которые считаются более важными для общества, такие как поставщики медицинских услуг, местные органы власти и другие хранители критически важной инфраструктуры ”.*

Если бы был введен запрет, мы считаем, что злоумышленники быстро изменили бы курс и перешли бы от высокоэффективных атак на основе шифрования к другим, менее разрушительным формам киберпреступности. Им действительно не имело бы смысла тратить время и усилия на атаки на организации, которые не могли заплатить. Кроме того, злоумышленники уже атакуют поставщиков медицинских услуг, местные органы власти и других хранителей критически важной инфраструктуры – неустанно, изо дня в день - и далеко не факт, что у них будет стимул или ресурсы для более частых атак.

Еще одна причина, которую часто выдвигают в качестве аргумента против запрета – и она также кратко упоминается в отчете Целевой группы, – заключается в том, что некоторые организации нарушат закон и все равно заплатят. Хотя это, скорее всего, верно, это не означает, что запрет не будет эффективным. Запрет не обязательно приведет к прекращению всех платежей, его просто нужно будет прекратить в достаточной степени, чтобы гарантировать, что программы-вымогатели перестанут приносить прибыль, и, поскольку большинство компаний будут соблюдать закон, это, вероятно, будет достигнуто.

Да, запрет платежей может вызвать проблемы в краткосрочной перспективе для некоторых жертв, но *не* их запрет вызывает еще больше проблем, причем в долгосрочной перспективе и для всех. Это гарантирует, что организации будут по-прежнему подвергаться атакам, что больницы, школы и государственные службы будут по-прежнему работать с перебоями, что экономический удар в США по-прежнему обойдется в несколько миллиардов долларов и, что наиболее важно, что программы-вымогатели по-прежнему будут представлять угрозу для жизни.

Конечно, есть и другие механизмы, которые можно было бы опробовать – и которые в настоящее время опробуются, – но они вряд ли окажут существенное влияние на объемы программ-вымогателей в краткосрочной перспективе. Запрет действительно является единственным быстрым решением.

Следует отметить, что запрет не будет беспрецедентным. В 2022 году и Северная Каролина, и Флорида запретили организациям государственного сектора оплачивать требования.[5] Насколько нам известно, ни одна организация ни в одном из штатов не столкнулась с катастрофической потерей данных в результате запрета и ни у одной не было необычно чрезмерных простоев.

Больницы

Программы-вымогатели, без сомнения, представляют угрозу для жизни. При неотложной медицинской помощи важна каждая секунда. Если доступ к лечению задерживается из-за необходимости перенаправить машины скорой помощи из больниц, где требуется выкуп, плохие исходы становятся более вероятными. Пациенты могут умереть или остаться с постоянной инвалидностью, чего можно было бы избежать при более быстром лечении.

Перенаправленные машины скорой помощи - не единственный риск для безопасности пациентов. Задержка с оформлением заявок и сдачей анализов, недоступность электронных медицинских карт и ошибки, связанные с ручным ведением записей, также могут негативно повлиять на результаты лечения. Например, в 2022 году 3-летнему пациенту, как сообщается, была введена “мегадоза” опиоидного обезболивающего в результате сбоя компьютерных систем больницы.[6] Частота таких инцидентов и их влияние на уход за пациентами и результаты лечения неизвестны.

Это также может повлиять на обслуживание пациентов в больницах, расположенных рядом с объектами, подвергшимися вымогательству. В исследовательском документе, опубликованном в мае 2023 года, был сделан вывод, что близлежащие больницы, которым необходимо принимать дополнительных пациентов, могут испытывать “ресурсные ограничения, влияющие на своевременное оказание помощи при таких состояниях, как острый инсульт. Эти результаты свидетельствуют о том, что целевые кибератаки на больницы могут быть связаны с перебоями в оказании медицинской помощи в нецелевых больницах в сообществе и должны рассматриваться как региональная катастрофа ”.[7]

В 2023 году программы-вымогатели затронули 46 больничных систем в общей сложности в 141 больнице, и по меньшей мере в 32 из 46 была украдена информация, включая защищенную медицинскую информацию.

Известные инциденты включали ноябрьскую атаку на Ardent Health Services – систему здравоохранения, состоящую из 30 больниц, - в результате которой больницы в трех штатах перенаправили машины скорой помощи.[8]

K-12 школ

По меньшей мере 108 округов K-12 пострадали от программ-вымогателей в 2023 году, что более чем вдвое превышает 45 округов, пострадавших в 2022 году. У нас нет объяснения такому увеличению. В пострадавших округах насчитывалось в общей сложности 1899 школ, и по меньшей мере в 77 из 108 были украдены данные.

Известные инциденты включали атаку на государственные школы Миннеаполиса, которая прервала обучение во многих школах округа и привела к размещению в Интернете почти 200 000 украденных файлов. Файлы содержали подробную информацию об изнасилованиях в кампусах и случаях жестокого обращения с учителями, психологические заключения студентов и другую чрезвычайно конфиденциальную информацию.[9]

Высшие учебные заведения

По меньшей мере 72 школы после окончания средней школы пострадали от программ-вымогателей, по сравнению с 44 в 2022 году и 26 в 2021 году. По меньшей мере в 60 из 72 были украдены данные.

Пострадавшие школы включали Гавайский университет, Университет Южного Арканзаса и Стэнфорд.

Правительства

В 2023 году были затронуты по меньшей мере 95 государственных организаций по сравнению со 106 в 2022 году. Хотя на основании публичных отчетов известно, что только у 60 из 95 были украдены данные, вполне вероятно, что это произошло у большинства, если не у всех.

Обратите внимание, что снижение связано с тем фактом, что в 2022 году в число 55 правительств штата Арканзас, которые пострадали в результате атаки на поставщика общих решений.[10] Если бы этот инцидент не учитывался для статистических целей, количество инцидентов в 2023 году увеличилось бы более чем на 50 процентов по сравнению с предыдущим годом.

Пострадавшие правительства включали города Даллас, Модесто и Окленд. Округ Сан-Бернардино выплатил выкуп в размере 1,1 миллиона долларов[11], в то время как другая жертва, город Лоуэлл, потратил 1 миллион долларов на кредитную защиту пострадавших лиц.[12]

В феврале Служба судебных приставов США подверглась атаке программ-вымогателей, в ходе которой была украдена “информация, относящаяся к субъектам расследований USMS, третьим сторонам и определенным сотрудникам USMS”.[13] Впоследствии данные, предположительно украденные из USMS, были выставлены на продажу на русскоязычном форуме по борьбе с киберпреступностью.[14]

Частный сектор

Занижение данных и намеренное запутывание затрудняют составление статистических данных об инцидентах, связанных с частным сектором. Из–за этого даже на самые элементарные вопросы, такие как общее количество инцидентов и процент жертв, которые платят, невозможно получить достоверный ответ.

Тем не менее, мы точно знаем, что в 2023 году список жертв затронул несколько компаний с известными именами, включая Boeing, MGM Resorts, Caesars Entertainment, DISH network и Johnson Controls.

Экономические последствия

Согласно обновлению Chainalysis за середину года, за первые шесть месяцев года было выплачено[15] 449 миллионов долларов выкупов, и 2023 год на сегодняшний день считается вторым по прибыльности годом для участников программы-вымогателя. Большая часть из этих 449 миллионов долларов, вероятно, была выплачена американскими организациями.

Другие расходы, связанные с программами-вымогателями, включают сбои в работе, реагирование на инциденты, потерю интеллектуальной собственности и множество других расходов после взлома, включая подачу документов в регулирующие органы и уведомления.

Хотя у нас недостаточно данных, чтобы оценить общую стоимость программ-вымогателей для экономики США, можно с уверенностью предположить, что она исчисляется миллиардами долларов. Для справки, MGM Resorts оценила стоимость сентябрьской атаки в 100 миллионов долларов,[16] в то время как августовская атака на Clorox на данный момент обошлась в 356 миллионов долларов.[16]

Следует отметить, что финансовые последствия программ-вымогателей не обязательно ограничиваются целевыми компаниями. Например, атаки на поставщиков решений и услуг могут нарушить работу их корпоративных клиентов, а также вызвать волновой эффект, который ощущается в более широком масштабе. В декабре около 60 кредитных союзов столкнулись с перебоями в работе в результате атаки на поставщика технологий, в результате чего клиенты, как сообщается, не смогли получить доступ к своим учетным записям.[17]

MOVEit

Инцидент с MOVEit представлял собой атаку, в ходе которой программа–вымогатель Cl0p использовала уязвимость нулевого дня для кражи данных через широко используемую платформу передачи файлов MOVEit. Инцидент затронул более 2600 организаций, в основном базирующихся в США, со многими жертвами в государственном секторе и сфере образования, и, возможно, обошелся в общую сумму около 15 миллиардов долларов.

Мы решили не подсчитывать пострадавшие организации для целей этого отчета, поскольку это сильно исказило бы цифры. Кроме того, инцидент не обязательно соответствует всеобщему определению понятия “программа-вымогатель”, поскольку никакие данные не были зашифрованы и не каждая пострадавшая организация получила требование о выкупе.

Подведение итогов

В 2018 году выплаты выкупа составляли в среднем 5 000 долларов,[18] но к 2023 году эта цифра увеличилась на 29 900 процентов и составила около 1,5 миллиона долларов.[19] Этот снежный ком стал ключом к резкому росту числа программ-вымогателей. Чем больше денег у участников программы–вымогателя - а сейчас у них на 29 900 процентов больше, чем было раньше, – тем больше они могут инвестировать в масштабирование своих операций, покупку zero days, а также покупку и подкуп для проникновения в сети. Это затрудняет их пресечение, и, если количество платежей продолжит расти, остановить их станет еще труднее.

Следует отметить, что тактика, используемая злоумышленниками, стала более экстремальной и, из-за количества денег, которые сейчас на кону, вероятно, станет еще более экстремальной. Например, в декабре сообщалось, что злоумышленник пытался оказать давление на онкологическую больницу с целью получения выкупа, угрожая прихлопнуть ее пациентов.[20] Прихлопывание - это использование полиции в качестве оружия: звонок в службу 911 с ложными сообщениями о преступной деятельности с целью вызвать реакцию, подобную команде спецназа, по целевым адресам. Эта практика привела к многочисленным травмам и смертям.[21] Возможность дальнейшей эскалации делает еще более важным принятие оперативных мер.

Наконец, крайне важно, чтобы правительства работали над пониманием условий, которые позволили программам-вымогателям быстро превратиться из простого неудобства в многомиллиардный кризис. Например, было ли киберстрахование причиной увеличения требований на 29 900 процентов, и если да, то как этого можно было избежать? Извлеченные уроки могут позволить более эффективно законодательно реагировать на будущие угрозы.

Ссылки

[1]Мы попытались количественно оценить, насколько вредны для пациентов атаки программ-вымогателей в больницах. Вот что мы обнаружили. https://www.statnews.com/2023/11/17/hospital-ransomware-attack-patient-deaths-study/

[2]Возглавляемая США коалиция по кибербезопасности клянется не платить требования хакеров о выкупе https://techcrunch.com/2023/10/31/united-states-cybersecurity-coalition-deny-ransom-demands

[3]Что это значит — проблемы группы программ-вымогателей CitrixBleed растут по мере взлома более 60 кредитных союзов, больниц, финансовых служб и многого другого в США https://doublepulsar.com/what-it-means-citrixbleed-ransom-group-woes-grow-as-over-60-credit-unions-hospitals-47766a091d4f

[4]Отчет RTF: Борьба с программами-вымогателями https://securityandtechnology.org/wp-content/uploads/2021/09/IST-Ransomware-Task-Force-Report.pdf

[5]Взгляд изнутри на усилия штатов по запрету государственных платежей с помощью программ-вымогателей https://therecord.media/an-inside-look-into-states-efforts-to-ban-govt-ransomware-payments

[6]3-летним детям дали слишком много обезболивающих после кибератаки, отключившей компьютеры MercyOne, говорят родители https://www.desmoinesregister.com/story/news/health/2022/10/13/apparent-ransomware-attack-mercyone-iowa-affects-hospital-patients/69553280007/

[7]Атак программ-вымогателей, связанных с перебоями в работе соседних отделений неотложной помощи в США https://pubmed.ncbi.nlm.nih.gov/37155166/

[8]отделений неотложной помощи по крайней мере в 3 штатах отвлекают пациентов после атаки программ-вымогателей https://www.nbcnews.com/tech/security/emergency-rooms-least-3-states-diverting-patients-ransomware-attack-rcna126890

[9]Психологических заключений студентов, заявлений о злоупотреблениях, просочившихся от хакеров-вымогателей https://www.nbcnews.com/tech/security/students-psychological-reports-abuse-allegations-leaked-ransomware-hac-rcna79414

[10]офисов округа Миллер пострадали от кибератаки https://www.ktbs.com/news/texarkana/miller-county-offices-impacted-by-cyber-attack/article_5e175af4-6794-11ed-96b8-53186a21f676.html

[11]Округ Сан-Бернардино платит 1,1 миллиона долларов за урегулирование атаки программ-вымогателей https://ktla.com/news/local-news/san-bernardino-county-pays-1-1-million-to-settle-ransomware-attack/

[12]Защита LifeLock обойдется Лоуэллу в 1 миллион долларов https://www.lowellsun.com/2023/05/25/lifelock-protection-to-cost-lowell-1-million/

[13]Служба судебных приставов США сталкивается с "серьезным" нарушением безопасности, которое компрометирует конфиденциальную информацию, говорят высокопоставленные представители правоохранительных органов https://www.nbcnews.com/politics/politics-news/major-us-marshals-service-hack-compromises-sensitive-info-rcna72581

[14]Хакеров, продающих данные, предположительно украденные в Службе судебных приставов США, взломали https://www.bleepingcomputer.com/news/security/hacker-selling-data-allegedly-stolen-in-us-marshals-service-hack/

[15]Кредитных союзов Hopewell пострадали от атаки программ-вымогателей, блокирующих доступ клиентов к учетным записям https://www.wric.com/news/taking-action/hopewell-credit-union-hit-by-ransomware-attack-blocking-customers-access-to-accounts/

[16]Обновление криптопреступности за середину года https://www.chainalysis.com/blog/crypto-crime-midyear-2023-update-ransomware-scams/

[17]MGMG Resorts International 8-K https://www.sec.gov/ix?doc=/Archives/edgar/data/789570/000119312523251667/d461062d8k.htm

[18]Кибератака компании Clorox в 2023 году: серьезные последствия, системные сбои и нехватка продукции https://thrivedx.com/resources/article/clorox-companys-2023-cyberattack-fallout

[19]Отчет о глобальном рынке программ-вымогателей https://static1.squarespace.com/static/5ab16578e2ccd10898976178/t/5bc541a4419202fbc6ce3434/1539654309673/Coveware+Global+Ransomware+Report.pdf

[20]Путей к запрету платежей с помощью программ-вымогателей https://www.centerforcybersecuritypolicy.org/insights-and-research/the-path-to-banning-ransomware-payments

[21]Недавние атаки на Фреда Хатча и Integris: становятся ли попытки прямого вымогательства у пациентов “новой нормой”? https://www.databreaches.net/recent-attacks-on-fred-hutch-and-integris-is-attempting-to-extort-patients-directly-becoming-the-new-normal/