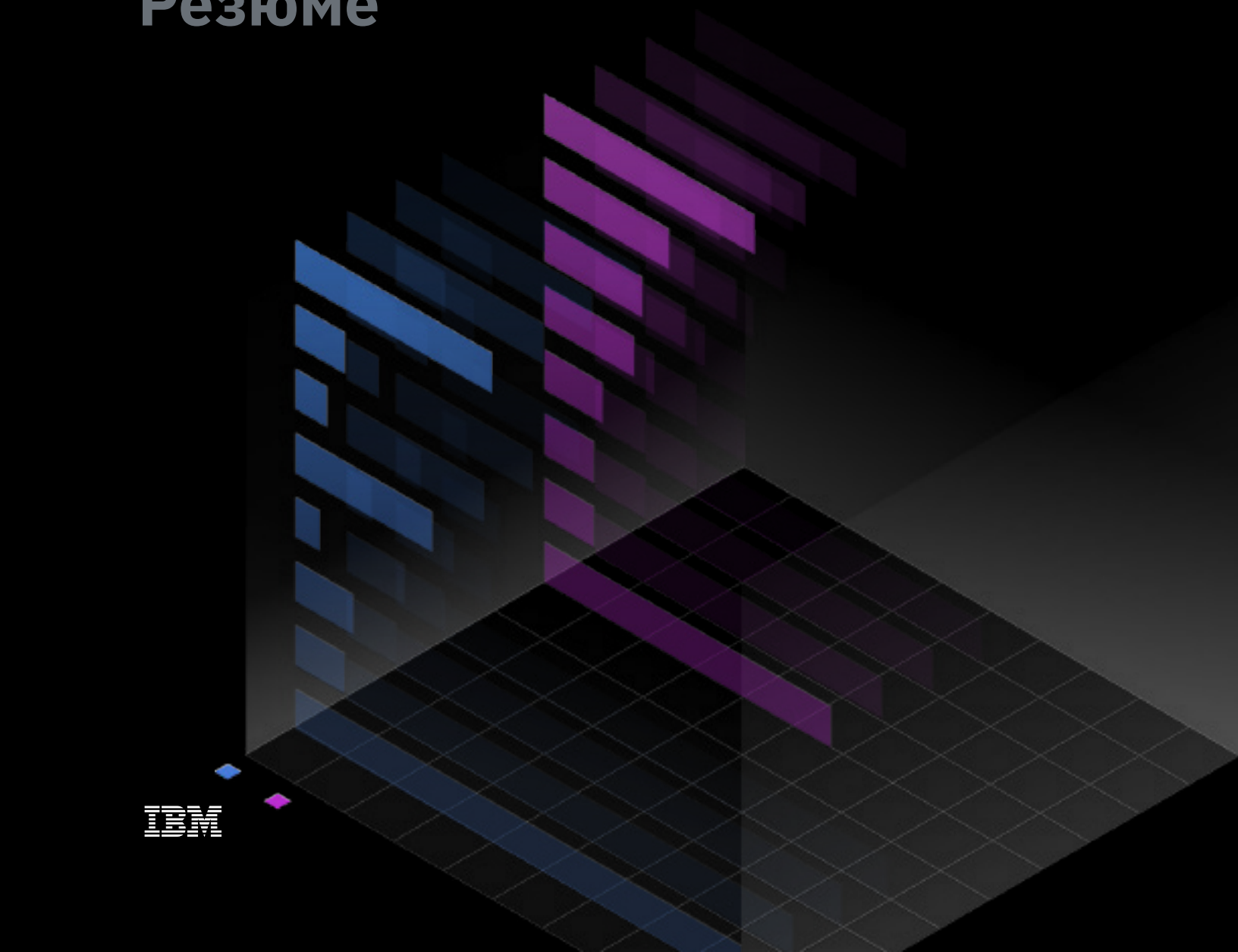
IBM Security

X-Force Threat Intelligence Index 2021

Резюме



IBM

Введение

Вне всяких сомнений, в нашей памяти 2020 год останется одним из самых необычных, и наполненных важными событиями, изменившими нашу привычную реальность. Глобальная пандемия, связанные с ней экономические потрясения, социальные и политические волнения затронули жизни миллионов людей. Отзвуки этих событий оказали глубокое влияние на коммерческие организации, и многие из них перешли на использование распределенных рабочих ресурсов.

Чрезвычайные обстоятельства 2020 года затронули и интернет-пространство. У киберпреступников появилась возможность использовать в своих интересах сети коммуникаций и сделать мишенью кибератак цепочки поставок и критически важную инфраструктуру. Год закончился тем же, с чего начался, — обнаружением глобальных угроз, требующих быстрого реагирования и устранения. Атаки, по большей части приписываемые действующим по указу государства субъектам, которые воспользовались обходными лазейками в ПО сетевого мониторинга для агрессивных действий против государственных и частных организаций, лишь подтвердили, что сторонних рисков следует ожидать, но их невозможно спрогнозировать.

Чтобы противостоять вызовам современного мира , IBM Security X-Force оценивает ландшафт киберугроз, помогает организациям разобраться в постоянно меняющихся технологиях, применяемых мошенниками, и связанных с ними рисках, а также в расстановке приоритетов принятия мер по обеспечению кибербезопасности. В дополнение к предоставляемой клиентам первоклассной аналитике угроз мы занимаемся анализом собираемых нами массивов данных для создания X-Force Threat Intelligence Index — ежегодного отчета о текущей картине угроз и ее изменениях.

Отслеживая тенденции, мы выявили, что масштабы программ-вымогателей продолжают расти, и данная угроза становится проблемой номер один, на которую в 2020 году приходилось 23 % устраненных X-Force нарушений безопасности. Участились случаи вымогания платежей злоумышленниками с использованием одновременно шифрования данных и угрозы слива персональной информации на общедоступные сайты. По оценкам X-Force, за счет подобных схем в 2020[1] году одной только группировке вымогателей удалось получить прибыль в размере свыше 123 миллионов долларов.

В 2020 году производственные организации подверглись натиску программ-вымогателей и многим другим видам атак. В целом, промышленность оказалась на втором месте среди отраслей, подвергшихся наибольшему количеству кибератак, уступив только сфере финансов и страхования. А в 2019 году она занимала восьмое место в этом рейтинге. X-Force удалось определить, что продвинутые злоумышленники использовали адресный фишинг в атаках на производственные предприятия и неправительственные организации, участвующие в цепочке поставок вакцины против COVID-19.

1. Все денежные расчеты приведены в долларах США.

Также злоумышленники постоянно совершенствовали вредоносные программы, особенно те, которые нацелены на ОС Linux с открытым исходным кодом, поддерживающую критически важную облачную инфраструктуру и хранилища данных. Анализ с помощью Intezer обнаружил 56 новых семейств вредоносных программ, разработанных в 2020 году для атаки на Linux. Это намного превышает темпы совершенствования других типов угроз.

Есть основания надеяться, что 2021 год будет лучше в этом отношении. Тенденции, как известно, трудно предсказать, но единственное, в чем мы можем быть уверены , — это перспектива дальнейших изменений. Обеспечение устойчивости к растущим вызовам кибербезопасности требует действенной аналитики и стратегического видения будущей более открытой и взаимосвязанной системы безопасности.

Руководствуясь принципами объединения усилий и взаимопомощи, подразделение IBM Security представляет отчет 2021 X-Force Threat Intelligence Index. Результаты этого отчета могут помочь сотрудникам служб информационной безопасности, специалистам по управлению рисками, лицам, отвечающим за принятие решений, аналитикам, средствам массовой информации и другим сторонам понять ландшафт киберугроз прошлого года и подготовиться к предстоящим вызовам.

Резюме

Служба IBM Security X-Force опиралась на огромное количество данных, полученных от наших клиентов и из общедоступных источников в период с января по декабрь 2020 года, для анализа типов атак, векторов заражения, а также сравнения отраслевых и глобальных тенденций. Ниже приведены некоторые из основных выводов, представленных в отчете X-Force Threat Intelligence Index.

23 %

Доля атак программ-вымогателей

Программы-вымогатели были самым популярным методом атак в 2020 году. На них приходилось 23 % всех инцидентов, на которые отреагировала и которые помогла устранить служба IBM Security X-Force.

Более 123 миллионов долларов

Ориентировочная прибыль от самой популярной программы-вымогателя

Согласно консервативным оценкам X-Force, одни только хакеры, использовавшие программу-вымогатель Sodinokibi (также известную как REvil), получили в 2020 году не менее 123 миллионов долларов прибыли и похитили около 21,6 терабайта данных.

25 %

Доля атак с наибольшей уязвимостью в первом квартале 2020 г.

В случае с компанией Citrix злоумышленники воспользовались обходом каталога. Эта уязвимость использовалась также в 25 % всех атак в первые три месяца года и в 8 % всех атак за 2020 год.

35 %

Доля систем сканирования уязвимостей с их последующим использованием в основных векторах заражения

Сканирование и использование уязвимостей стали основным вектором заражения в 2020 году, превзойдя фишинг, который был основным вектором в 2019 году.

#2

Место промышленного производства среди сфер, наиболее подверженных атакам

Промышленность стала второй наиболее атакуемой отраслью в 2020 году, поднявшись с восьмого места в 2019 году и уступив только сфере финансовых услуг.

5 часов

Продолжительность обучающих видеоматериалов по организации атак, найденных на сервере группировки злоумышленников

Операционные ошибки иранских злоумышленников, действующих по указу государства, позволили исследователям службы X-Force обнаружить на неправильно сконфигурированном сервере видеоматериалы длительностью около 5 часов и понять, какие технологии используют злоумышленники.

100+

Количество должностных лиц, ставших жертвами адресного фишинга

В середине 2020 года служба X-Force раскрыла глобальную фишинговую кампанию, которая затронула более 100 высокопоставленных лиц, руководивших приобретением средств индивидуальной защиты (СИЗ) для борьбы с COVID-19.

49 %

Темпы роста уязвимостей АСУ ТП в 2019–2020 гг.

Уровень уязвимостей, обнаруженных в 2020 году и связанных с автоматизированными системами управления технологическими процессами (АСУ ТП), на 49 % превысил аналогичный показатель 2019 года.

56

Количество новых семейств вредоносных программ для Linux

В 2020 году было обнаружено 56 новых семейств вредоносных программ, созданных для Linux, что является самым высоким показателем за всю историю. Это на 40 % больше по сравнению с 2019 годом.

31%

Европейская доля атак

Европа стала регионом, наиболее подверженным атакам в 2020 году: на нее пришлось 31 % зафиксированных службой X-Force атак. За ней следуют Северная Америка (27 %) и Азия (25 %).

Перспективы на будущее

В 2021 году сочетание старых и новых угроз потребует от команд безопасности одновременного рассмотрения множества рисков. Вот некоторые из основных выводов от аналитиков X-Force относительно приоритетов на текущий год:

— **В 2021 году объемы рисков будут продолжать расти.** Будут возникать тысячи новых уязвимостей как в старых, так и в новых приложениях и устройствах.

— **Тенденция двойного вымогательства с помощью программ-вымогателей, вероятно, сохранится на протяжении 2021 года.** Угрожая сливом украденных данных на неблагонадежных веб-сайтах, злоумышленники устанавливают более высокую цену за то, чтобы избежать заражения программами-вымогателями.

— **Злоумышленники продолжают переключаться между разными векторами атак.** Целенаправленные атаки на системы под управлением ОС Linux, операционные технологии (OT), устройства Интернета вещей и облачные среды будут продолжаться. По мере совершенствования этих систем и устройств злоумышленники могут быстро переключаться на другие направления, особенно после громких инцидентов.

— **В каждой отрасли есть свои риски.** Ежегодное изменение злоумышленниками атакуемых отраслей лишь подтверждает существование риска для всех индустрий и необходимость всестороннего развития и совершенствования программ кибербезопасности.

Рекомендации по устойчивости

Согласно наблюдениям IBM Security X-Force, приведенным в этом отчете, постоянное отслеживание угроз безопасности и создание надежных средств реагирования являются эффективными способами смягчения угроз на меняющемся ландшафте, независимо от того, в какой отрасли или стране эти угрозы возникают.

X-Force рекомендует организациям предпринять следующие меры, чтобы лучше подготовиться к киберугрозам в 2021 году:

Лучше действовать на опережение, чем реагировать на угрозу. Внедрите аналитику угроз, чтобы лучше понимать мотивы и тактику злоумышленников и правильно распределять ресурсы безопасности.

Подготовка — это ключ к успеху реагирования на угрозу программ-вымогателей. Планирование действий на случай атаки программ-вымогателей, в том числе план по устранению комбинированных программ и методов хищения данных, а также регулярное тестирование этого плана могут существенно повлиять на эффективность мер реагирования вашей организации в критический момент.

Дважды проверяйте структуру процесса управления исправлениями в вашей организации. Поскольку сканирование уязвимостей и их последующее использование стали наиболее распространенным вектором заражения в прошлом году, займитесь укреплением защиты своей инфраструктуры и активизируйте внутренние средства обнаружения, чтобы быстро и эффективно идентифицировать и пресекать попытки автоматизированного злонамеренного проникновения.

Защититесь от внутрисистемных угроз. Задействуйте решения для предотвращения потери данных (data loss prevention, DLP), а также обучение и мониторинг, чтобы предотвратить проникновение случайных лиц или злоумышленников в вашу корпоративную сть.

Создайте и обучите команду реагирования на инциденты внутри вашей организации. Если такой возможности нет, задействуйте эффективный механизм для оперативного реагирования на наиболее опасные инциденты.

Протестируйте устойчивость плана реагирования на инциденты в вашей организации, чтобы довести его осуществление до автоматизма. Теоретические тренинги или занятия в рамках киберполигона дадут вашим сотрудникам важный опыт, позволяющий сократить время реагирования, простоя и, в конечном итоге, сэкономить деньги в случае проникновения злоумышленников.

Внедрите многофакторную аутентификацию (MFA). Добавление дополнительных уровней защиты учетных записей продолжает оставаться одним из наиболее эффективных приоритетов в системах безопасности организаций.

Создавайте, тестируйте и храните резервные копии в автономном режиме. Не только наличие резервных копий, но и обеспечение их эффективност и путем тестирования в реальных условиях имеют решающее значение для безопасности организации. Это подтверждают данные за 2020 год, свидетельствующие о возобновлении активности программ-вымогателей.

Об IBM Security X-Force

IBM Security X-Force предоставляет возможности анализа, обнаружения и реагирования, чтобы помочь клиентам повысить уровень безопасности.

IBM Security X-Force Threat Intelligence объединяет телеметрию операций безопасности IBM, исследования, анализ реагирования на инциденты, коммерческие данные и открытые источники, чтобы помочь клиентам определять возникающие угрозы и в быстро принимать обоснованные решения в области безопасности.

Кроме того, хорошо обученная команда X-Force Incident Response помогает разработать стратегию устранения уязвимостей, что позволяет организациям более эффективно контролировать инциденты и утечку данных.

X-Force в сотрудничестве с киберполигоном IBM Security Command Center занимается подготовкой клиентов к реалиям современных угроз.

В течение года исследователи IBM X-Force также предоставляют результаты текущих исследований и аналитические отчеты в форме блогов, официальных документов, публикаций и подкастов, чтобы акцентировать наше внимание на наиболее продвинутых угрозах, новых вредоносных программах и новых методах атак. Кроме того, большой объем актуальных аналитических материалов доступен нашим клиентам по подписке на платформе Premier Threat Intelligence.

Сделайте следующий шаг

Узнайте, как усовершенствовать систему реагирования на инциденты с помощью IBM Security >

Об IBM Security

IBM Security работает вместе с вами над защитой вашего бизнеса с помощью расширенного и интегрированного портфолио продуктов и услуг корпоративной безопасности с использованием возможностей искусственного интеллекта. Это обеспечивает современный подход к вашей стратегии безопасности на принципах «нулевого доверия» и помогает вам успешно работать даже в неопределенных условиях. Согласовывая стратегию безопасности с вашим бизнесом, интегрируя решения, предназначенные для защиты ваших цифровых пользователей, активов и данных, и развертывая технологии управления защитой от растущих угроз, мы помогаем вам управлять рисками, возникающими в современных гибридных облачных средах.

Наш новый современный открытый подход — платформа IBM Cloud Pak for Security . Она построена на базе RedHat Open Shift и поддерживает современные гибридные мультиоблачные среды, предусматривающие обширную партнерскую экосистему. Cloud Pak for Security — это готовое к работе контейнерное программное решение, которое позволяет вам управлять безопасностью ваших данных и приложений, оперативно интегрируя существующие инструменты безопасности для более глубокого анализа угроз в гибридных облачных средах и сохраняя ваши данные там, где они изначально находятся. Это позволяет легко организовать и автоматизировать реагирование на инциденты.

Для получения дополнительной информации посетите сайт www.ibm.com/security, подпишитесь на @IBMSecurity в Твиттере или посетите блог IBM Security Intelligence.

Соавторы

Ведущий автор:
Камилла Синглтон

Авторы:
Эллисон Викофф Ари Эйтан
(Intezer) Чарльз Дебек
Шарлотта Хаммонд Чента Ли
Крис Сперри Кристофер
Кифер Клэр Забоева Дэвид
Макмиллен Дэвид Моултон
Дирк Хартц Джорджия

Прасинос Ян Галлахер (Intezer)
Джон Зорабедян Джошуа Чанг
Келли Кейн Лорен Дженсен
Лимор Кессем Марк Ашер
Мартин Стейгеманн Мэтью
ДеФир Меган Радогна
Мелисса Фридрих Мишель

Альварес Митч Мэйн
Ник Россман Пэтти
Кэхилл-Ингрэм
Рэндалл Росси Ричард
Эмерсон Салина
Ваттке Скотт Крейг
Скотт Мур

IBM Восточная Европа/Азия
123112 Москва
Пресненская наб., 10

Тел.: +7 (495) 775-8800
Февраль 2021 г.

IBM **Security**