IBM X-Force отчет 2022

Угрозы Информационной Безопасности

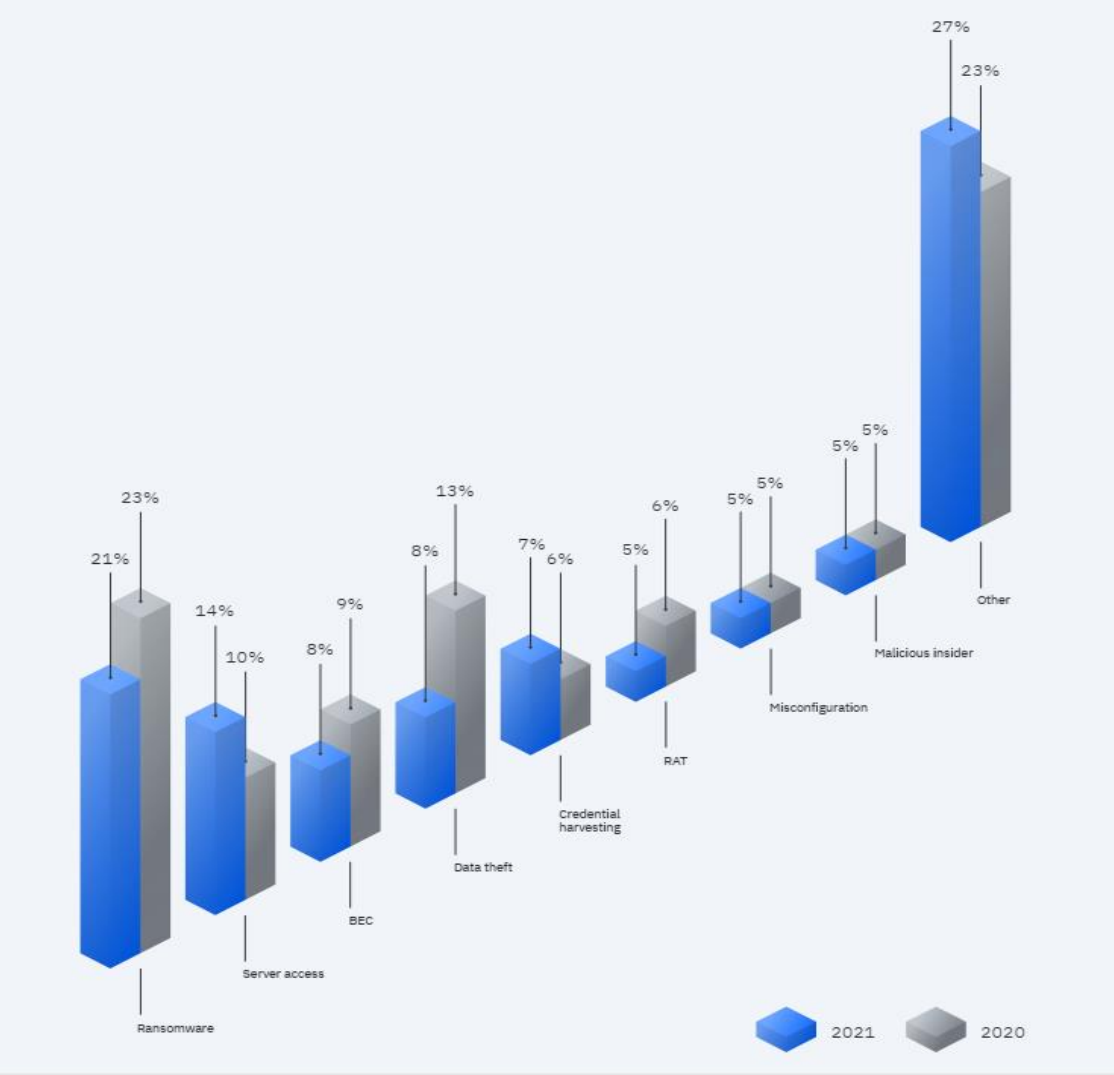
Who is X-Force?

- Каждый год IBM Security X-Force — команда экспертов и посредников в области кибербезопасности — анализирует миллиарды точек данных, чтобы выявить самые актуальные на сегодняшний день статистические данные и тенденции в области безопасности.
- Благодаря глубокому пониманию того, как субъекты угроз думают, разрабатывают стратегию и наносят удары, команда X-Force знает, как предотвращать, обнаруживать, реагировать на инциденты информационной безопасности и как восстанавливаться после инцидентов

Индекс аналитики угроз X-Force 2022

- В 2022 году Индекс аналитики IBM Security X-Force отмечает, что по мере того, как предприятия, учреждения и правительства продолжают адаптироваться к быстро меняющемуся глобальному рынку, включая гибридные и облачные рабочие среды, злоумышленники по-прежнему умеют использовать такие изменения.

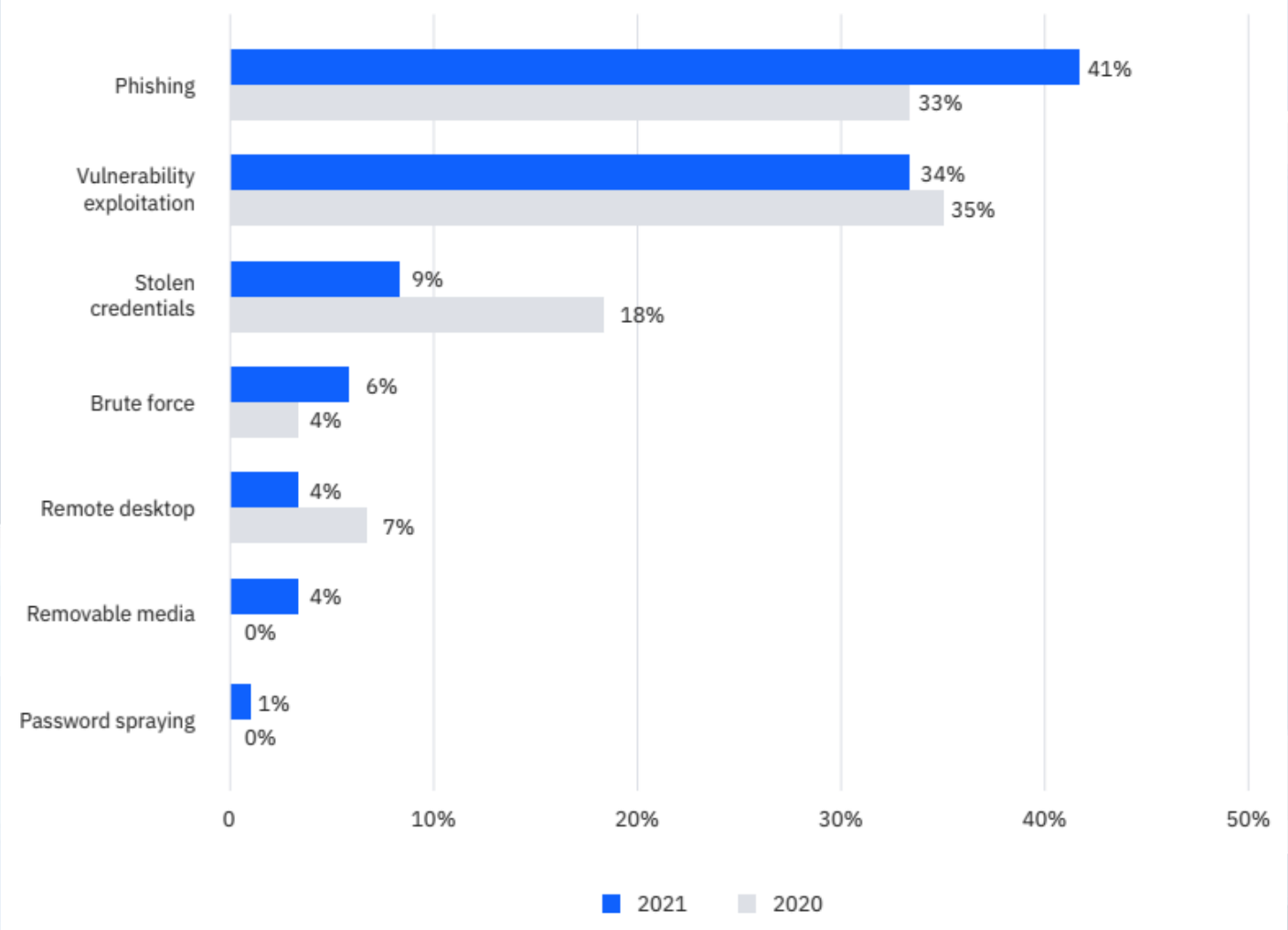
Основные типы атак в 2021 в сравнении с 2020



Тип атаки	2021	2020
Программы -вымогатели	21%	23%
Доступ к серверу	14%	10%
Компрометация e-mail	8%	9%
Хищение данных	8%	13%
Похищение учетных данных	7%	6%
Средства удаленного доступа	5%	6%
Ошибки конфигурации	5%	5%
Злонамеренный сотрудник	5%	5%
Прочие атаки*	27%	23%

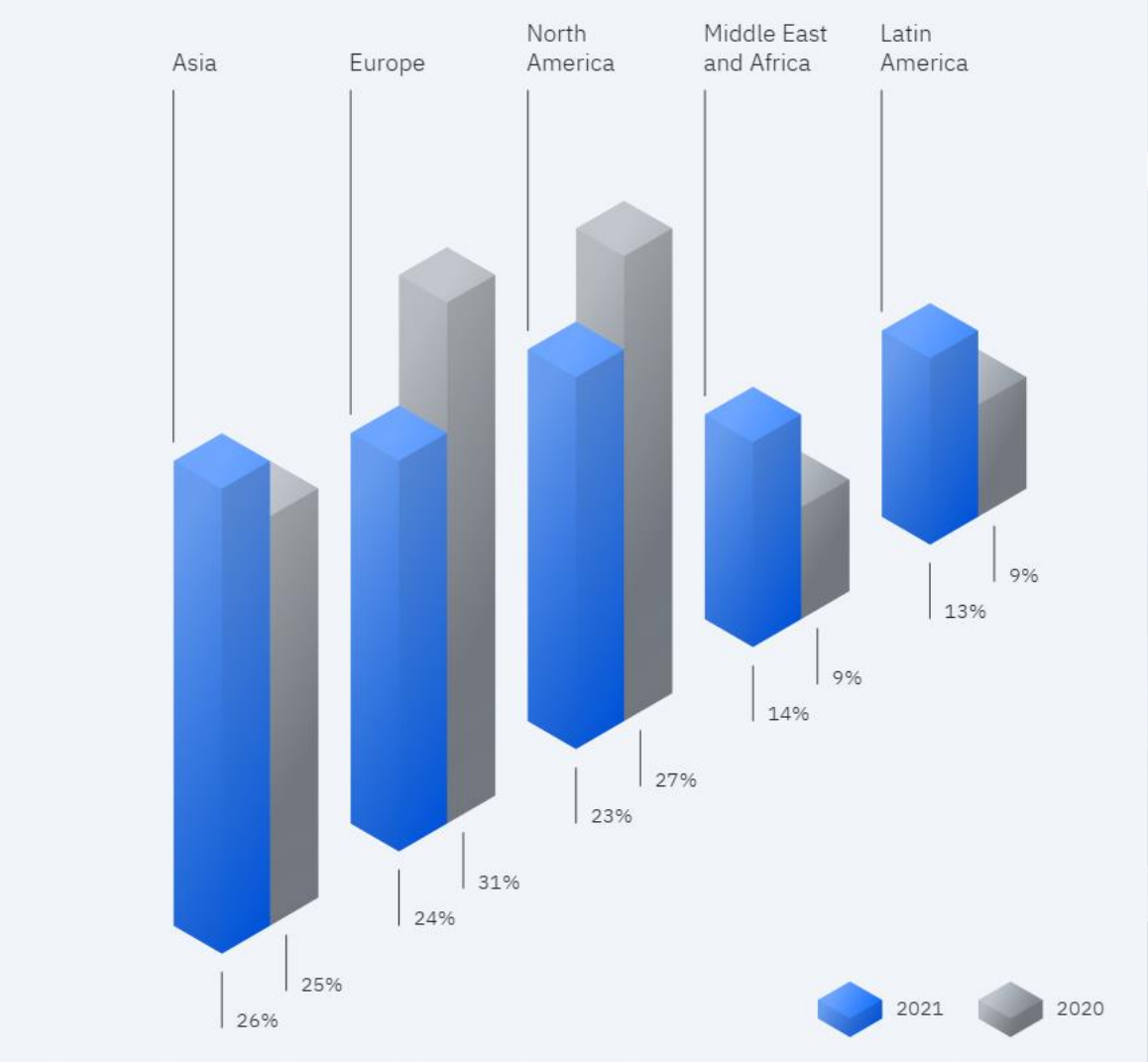
* Прочие атаки: рекламное ПО, банковские трояны, ботнеты, вредоносные криптомайнеры, подмена вэб станицы, мошенничество, DDoS, вредоносное ПО для точек продаж и POS терминалов, спам, внедрение вредоносного кода на вэб страницы, вэб оболочки и черви.

Основные векторы инфицирования в 2021 году в сравнении с 2020



Способ инфицирования	2021	2020
Фишинг	41%	33%
Использование уязвимостей	34%	35%
Похищение учетных данных	9%	18%
Взлом пароля	6%	4%
Средства удаленного доступа	4%	7%
Съемные носители	4%	0%
Распыление пароля	1%	0%

Распределение атак по регионам в 2021 году в сравнении с 2020



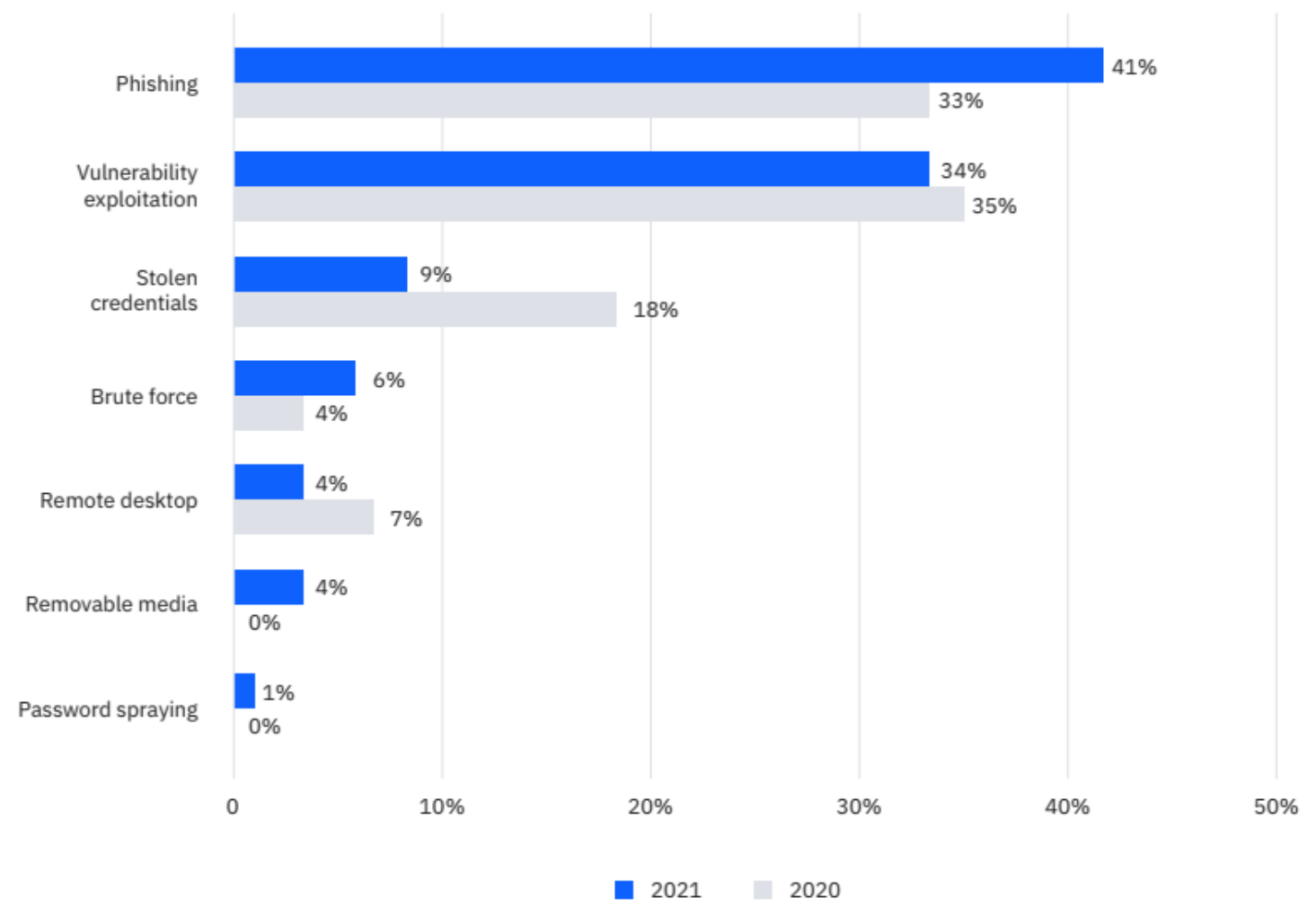
Регион	2021	2020
Азия	26%	25%
Европа	24%	31%
Северная Америка	23%	27%
Средний Восток и Африка	14%	9%
Латинская Америка	13%	9%

Производство становится самой атакуемой отраслью в мире.

- Впервые за пять лет производство опередило финансы и страхование по количеству кибератак, совершенных против этих отраслей, что усугубило проблемы с глобальными цепочками поставок. Производители плохо переносят простои, а субъекты программ-вымогателей извлекают выгоду из операционных стрессов, усугубленных пандемией.
- Каждая четвертая атака на этот сектор производится со стороны программ-вымогателей

Злоумышленники понимают, какую решающую роль играет производство в глобальных цепочках поставок, и стремятся разрушить эти организации

Основные векторы внедрения инфекций.

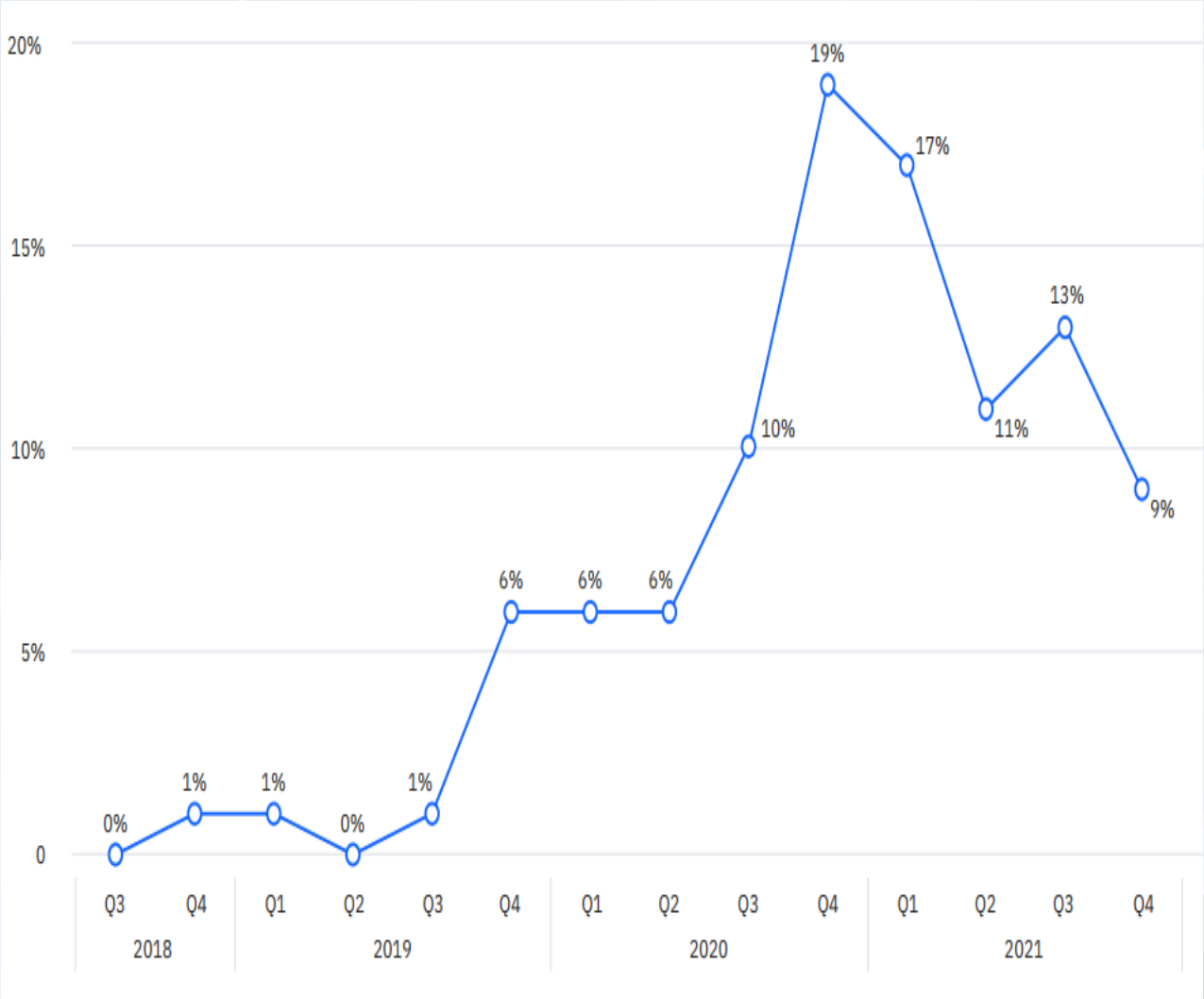


- 47% - использование уязвимостей
- 7% - съемные носители
- 40% - фишинг
- 3% - похищенные учетные данные
- 3% - взлом

Наиболее интенсивно атакуемые отрасли индустрии в 2021 году

Индустрия	Азия	Европа	Северная Америка	Средний Восток и Африка	Латинская Америка
Финансы и страхование	30%	18%		48%	15%
Промышленное производство	29%	25%	28%		22%
Профессиональные и бизнес-услуги	13%	15%	15%		
Розничная и оптовая торговля			11%		20%
Здравоохранение				15%	
Энергетика				10%	

Возрастание активности вредоносного ПО Интернета вещей



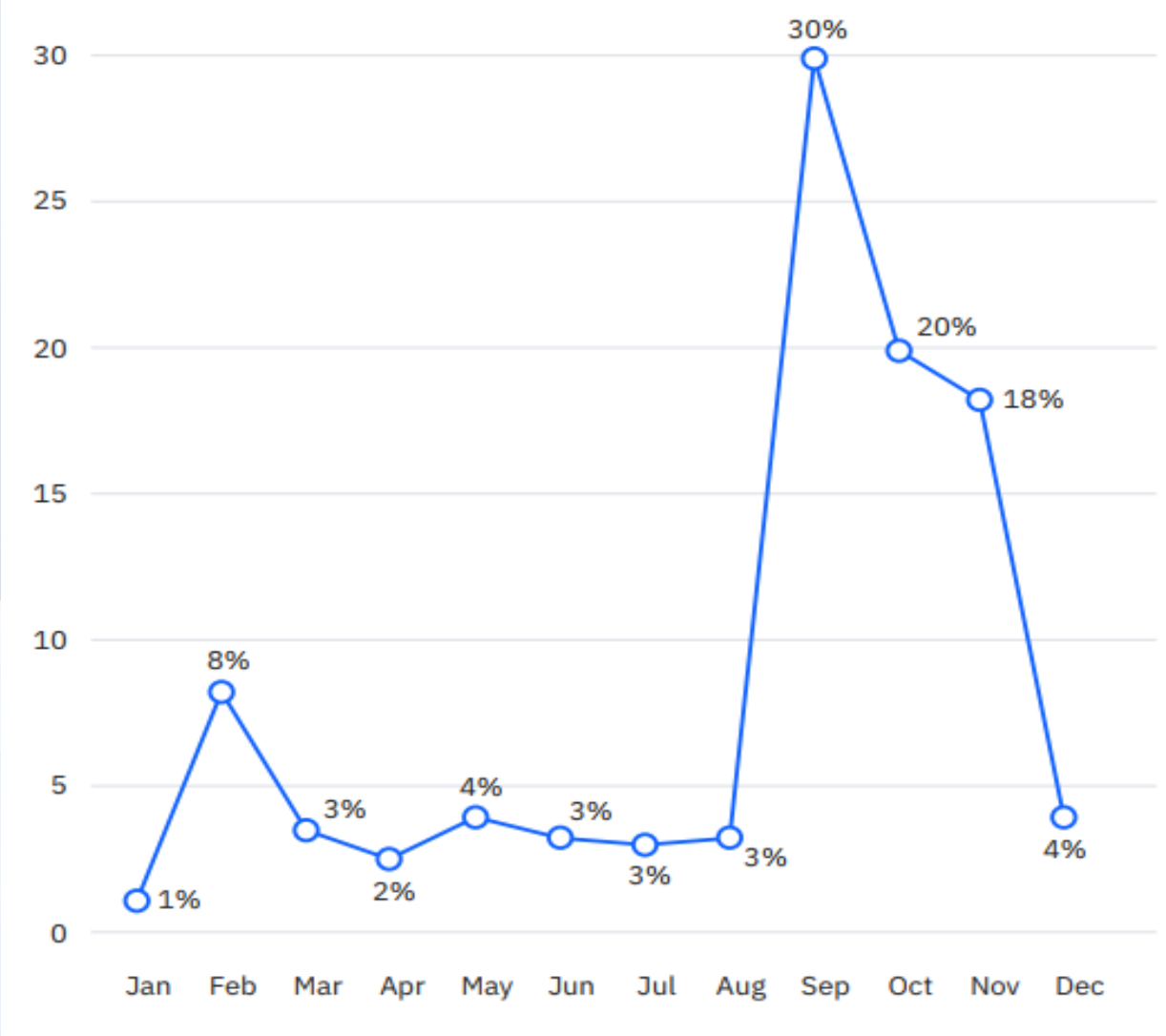
В период с 3-го квартала 2019 года по 4-й квартал 2020 года рост активности вредоносного ПО для Интернета вещей составил 3000%.

По мере укрепления защиты вредоносное ПО становится все более инновационным. Злоумышленники все чаще используют облачные службы обмена сообщениями и хранилища, чтобы маскировать свой вредоносный трафик в объеме легального трафика. А некоторые группы экспериментируют с новыми методами шифрования и запутывания кода, чтобы остаться незамеченными.

Количество уязвимостей, связанных с устройствами Интернета вещей, увеличилось в 2021 голу на 16% по сравнению с прошлым годом, при темпе роста для уязвимостей в целом всего 0,4%.

Поддержание должным образом защищенных систем, внедрение эффективных политик паролей и обеспечение соблюдения политик имеют решающее значение для поддержания надежного состояния безопасности в облаке.

Возрастание активности злоумышленников нацеленной на системы SCADA



Анализ данных 2021 года зафиксировано проведение злоумышленниками массированных разведывательных кампаний против средств связи промышленных сетей. В частности, в 2021 году наблюдался значительный рост в активности, нацеленной на TCP порт 502.

Порт 502 используется открытым протоколом Modbus для для обеспечения связи между серверами, шинами данных и программируемыми устройствами логических контроллеров (ПЛК) в промышленных сетях контроля и сбора данных (SCADA - Supervisory Control And Data Acquisition). Получение доступа к Modbus может позволить злоумышленникам управлять физическими устройствами, подключенными к Интернет.

В период с января по сентябрь 2021 г. увеличение активности, нацеленной на TCP порт 502 составило 2204%, а рост уязвимостей промышленных систем управления составил в 2021 году 50%, что представляет повышенный риск для производственного и энергетического секторов

Любая организация, использующая IoT, все чаще подвергается уязвимостям.

Новый тренд - Тройное Вымогательство

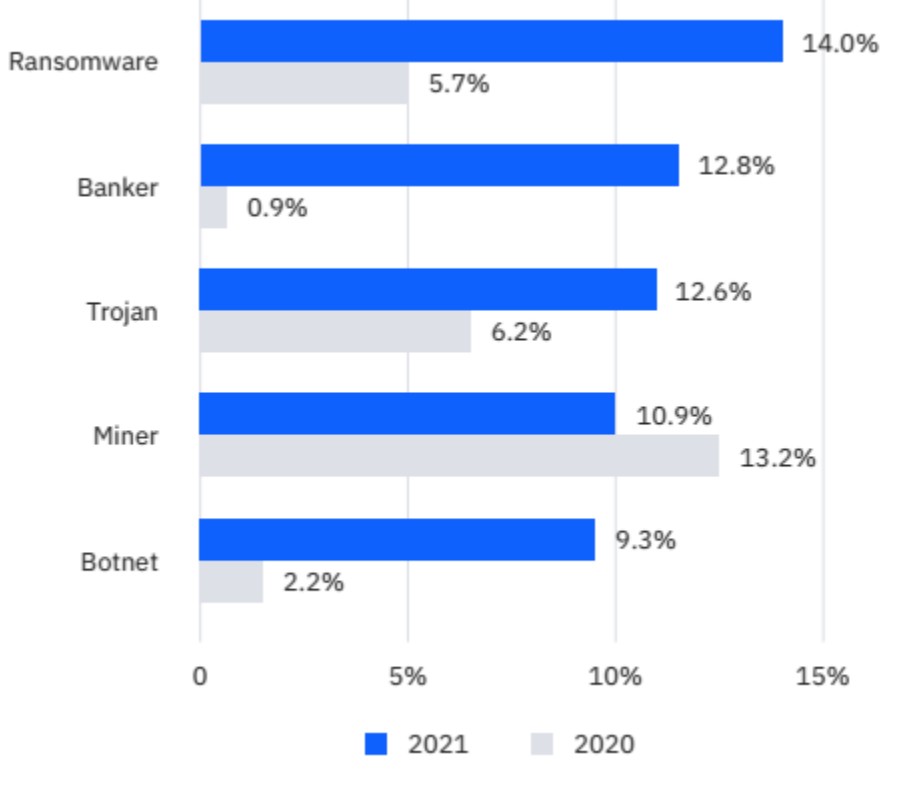
Новой тенденцией вымогателей стало расширение тактики «тройного вымогательства».

При этом типе атак субъекты угроз шифруют и крадут данные, а также угрожают совершить распределенную атаку типа «отказ в обслуживании» (DDoS) против пострадавшей организации.

Такого рода атаки особенно проблематичны для организаций, поскольку их сети оказываются заложниками двух видов вредоносных атак - часто одновременно - и затем становятся жертвами кражи (и часто утечки) данных.

Банды вымогателей начинают искать деловых партнеров своей основной жертвы, чтобы заставить их заплатить выкуп, чтобы предотвратить утечку собственных данных или сбои в бизнесе, вызванные атакой вымогателей.

Увеличение уникального вредоносного кода для Linux



Вредоносное ПО Linux выросло в 2021 году четырех из пяти категорий по сравнению с предыдущим годом, при этом наибольший рост наблюдался в банковских троянах, в которых инновации выросли более чем в десять раз.

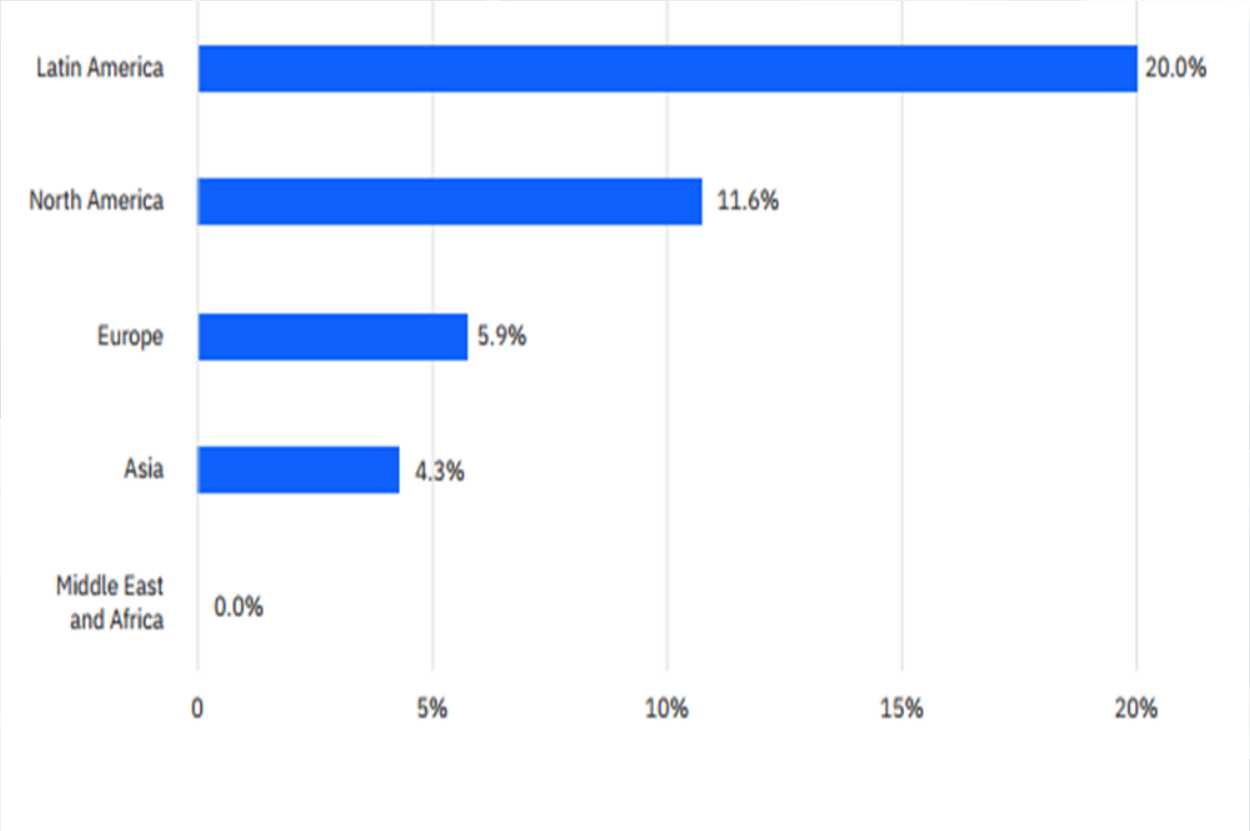
Категория вредоносного ПО	2021	2020
Ransomware (программы вымогатели)	14%	5,7%
Banker (кража учетных записей интернет-банкинга):	12,8%	0,9%
Trojan (вредоносное ПО, маскирующееся под легитимное)	12,6%	6,2%
Botnet (сеть с управляемыми удаленно автономными ботами)	9,3%	2,2%

Уровень инноваций вредоносного ПО Linux приблизился к уровню вредоносного ПО Windows и эта тенденция наблюдается и в 2022 году.

Увеличение кода для Linux может быть связано с тем, что организации все чаще переходят в облачные среды, которые часто полагаются на Linux, а злоумышленники следуют за ними.

Многофакторная аутентификация как метод снижения рисков

Процент инцидентов с компрометацией корпоративной электронной почты в общем числе инцидентов в 2021 году



В Латинской Америке, 20% атак были произведены через компрометацию корпоративной электронной почты. В 2019 году было 0%.

Многофакторная аутентификация (MFA) может снизить риск нескольких различных типов атак, включая программы-вымогатели, кражу данных, компрометацию корпоративной электронной почты (BEC - Business Email Compromise) и доступ к серверу. Но BEC растет в регионах, где MFA, по-видимому, менее распространен, например, в Латинской Америке.

Исследование X-Force подтверждает, что принципы нулевого доверия могут снизить подверженность организаций BEC. Технологии управления идентификацией и доступом упрощают реализацию MFA.

Крупные бренды — это билет на доступ в вашу организацию.

Фишинг (вишинг) был основным вектором заражения в 2021 году, а бренды, которые больше всего имитировались в наборах для фишинга, входят в число крупнейших и пользующихся наибольшим доверием компаний. Расследование X-Forceпоказало, что:

Топ 11 брендов использовавшихся для спуффинга и фишинговых атак в 2021 году

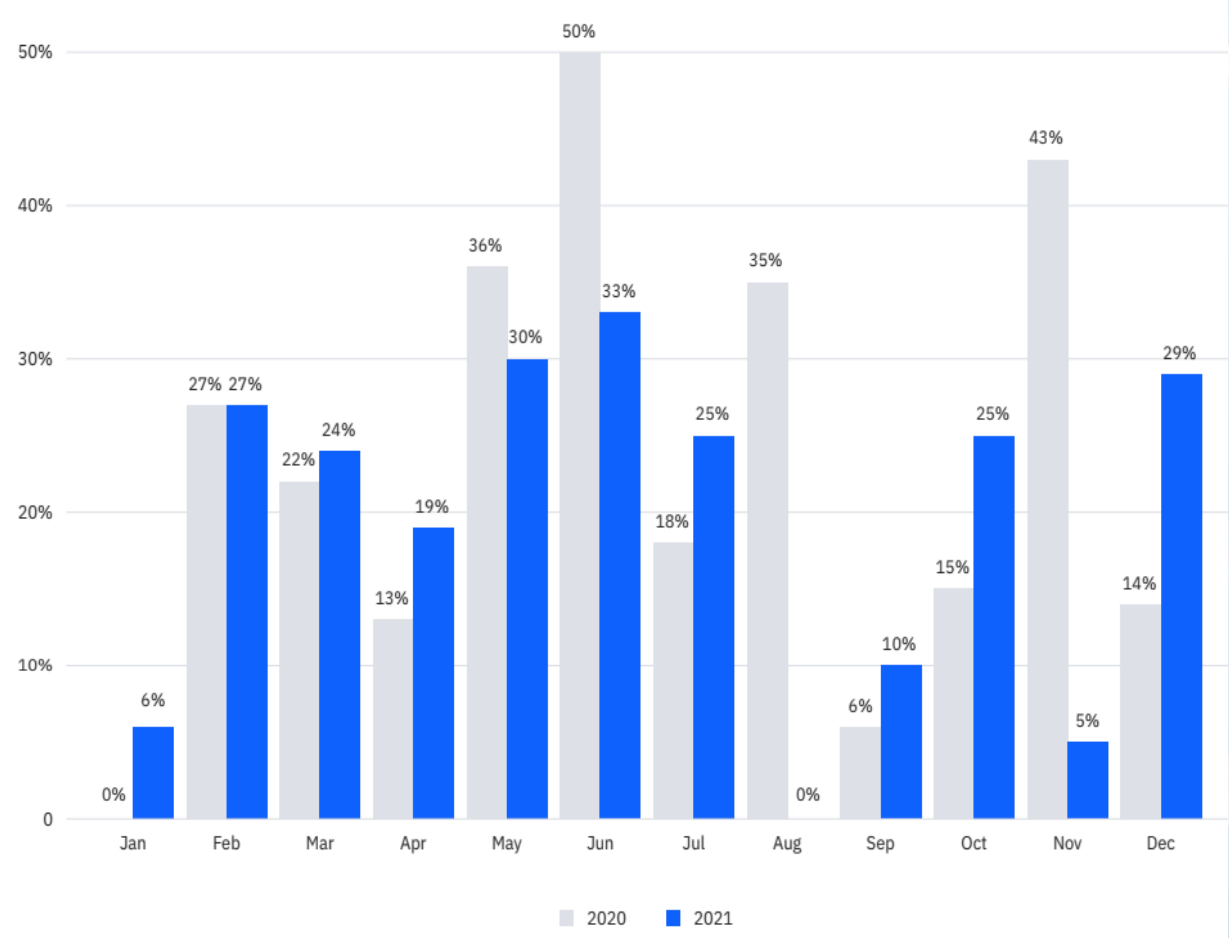
1. Microsoft
2. Apple
3. Google
4. BMO Harris Bank (BMO)
5. Chase
6. Amazon
7. Dropbox
8. DHL
9. CNN
10. Hotmail
11. Facebook

- Фишинговая атака обычно имела короткий срок жизни, причем почти треть длилась не дольше суток. В некоторых случаях индивидуальное развертывание фишинговой атаки длилось всего семь-восемь часов, прежде чем большинство хостинг-провайдеров идентифицировали сайт как вредоносный и блокировали его.
- Каждая атака в среднем собирала не более 75 потенциальных жертв, посетивших объект.
- Фишинговые наборы запрашивали учетные данные пользователя (комбинации email/ID/password) почти во всех наблюдаемых наборах (около 100%), за которыми следовали по популярности данные кредитных карт (61% запросов), почтовый адрес (40%), номер телефона (22%), дата рождения (17%), номер удостоверения личности (15%), вопросы безопасности (14%) и PIN-коды банкоматов (3%).
- Более 50% жертв, которые нажимали на ссылки фишинговых кампаний с добавленными телефонными звонками (вишинг или голосовой фишинг).
- Добавление вишинга (или голосового фишинга) к целевой фишинговой кампании в три раза эффективнее, чем классическая фишинговая кампания.
- Примерно каждый пятый сотрудник организации не может отличить поддельное электронное письмо от настоящего

Чтобы завоевать доверие, достаточно хорошо имитируемого логотипа..

Программы вымогатели являются ведущим типом атак

Количество реакций на инциденты в которых были задействованы программы-вымогатели в процентах к общему числу реакций по месяцам 2020-2021 годов



Средняя продолжительность жизни организованных групп вымогателей до ребрендинга или расформирования составляет 17 месяцев.

Программы-вымогатели остаются ведущим типом атак, хотя их доля в общем числе атак снизилась. По версии X-Force это является следствием деятельности правоохранительных органов. На операции группы киберпреступников REvil приходились колоссальные 37% атак программ-вымогателей, которые X-Force устранила в прошлом году, прежде чем банда закрылась в октябре 2021 года. Частота атак программ-вымогателей имеет тенденцию меняться в течение года, часто увеличиваясь в мае и июне. Атаки программ-вымогателей, по-видимому, снижаются в конце лета или начале осени, а в январе наблюдается наименьшая активность.

Имейте план реагирования на программы-вымогатели, резервные копии и альтернативное местоположение для важных бизнес-операций. Подумайте, сможете ли вы когда-нибудь заплатить выкуп.

X-Force Threat Intelligence Index 2022 Full Report

https://www.ibm.com/downloads/cas/ADLMYLAZ

Благодарю за внимание!

Ронжин В.В.
Для группы компаний «Nihol»
9 Декабря 2022г.