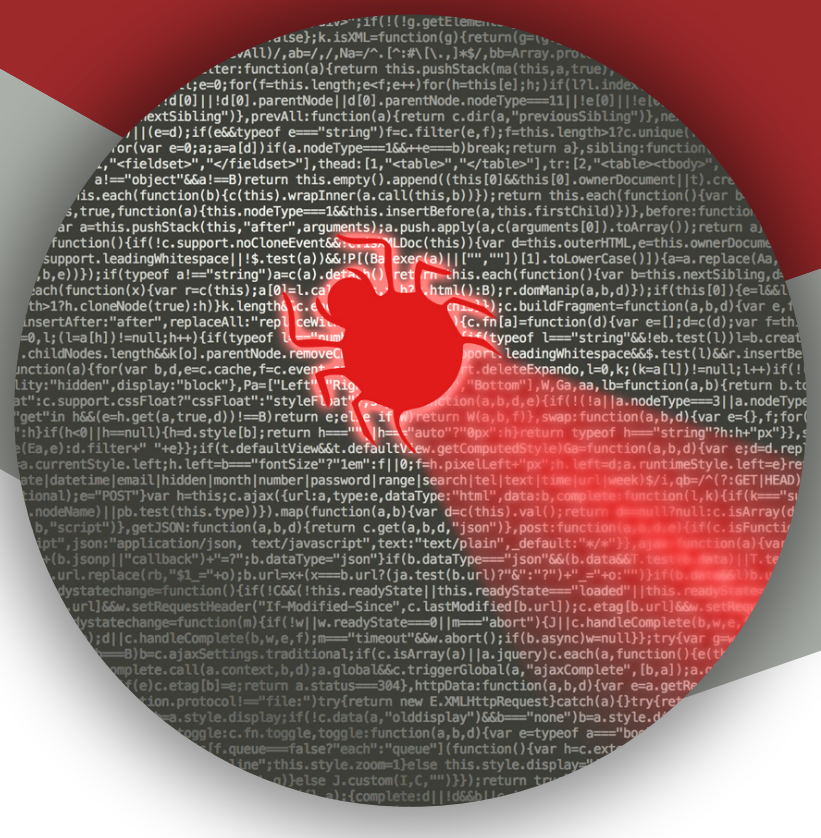
КИБЕР РИСКИ И УГРОЗЫ 2022-2023



@radiobailanys
t.me/radiobailanys

7 февраля 2023г. – второй день второй недели февраля

Всемирный день безопасного Интернета

Самое подходящее время поговорить о безопасности в новом дивном цифровом мире, который не смотря на свои многочисленные достоинства таит в себе много угроз и рисков.

Тема всегда была интересной и актуальной, но 2020 год сделал ее, одной из самых животрепещущих.

Немного цифр

Массовый переход в онлайн в 2020 году спровоцировал рост киберпреступлений на 358% по сравнению с 2019 годом.

В 2021 году преступлений в сети совершено на 125% больше чем в 2020. Каждый час в мире жертвами утечек данных становилось 97 человек.

За первой полугодие 2022 году было зарегистрировано 236,1 миллиона атак программ-вымогателей; каждый пятый пользователь Интернета открыл письмо с вредоносной ссылкой.

За 2022 год Meta обнаружила более 400 вредоносных приложений для iOS и Android, нацеленных на мобильных пользователей, чтобы украсть их учетные данные для входа в Facebook.

По оценке Федерально бюро расследований 53,35 миллиона граждан США пострадали от киберпреступлений в первой половине 2022 года.

50% организаций в США имеют полную страховку от киберугроз. Еще 28% имеют киберстрахование с исключениями или исключениями в полисе, что означает, что они не могут быть застрахованы от определенных атак или при определенных обстоятельствах.

1 из 10 организаций США (12%) не имеют никакой защиты от кибератак, рискуя получить финансовый крах в случае атаки.
Киберпреступления обходятся мировой экономике примерно в 787 671 доллар в час в 2021 году. В течение года это составляет 6 899 997 960 долларов

Тренды и прогнозы 2022/2023

Компания Group-IB в своем отчете «Эволюция киберпреступности. Анализ, тренды и прогнозы 2022/2023» назвала основные угрозы безопасноти для бизнеса:

Шифровальщики по прежнему остаются киберугрозой №1

Специалисты отмечают, что усложнение структур преступных группировок, и это усложнение все больше напомнинает структуру легальных ИТ-стартапов со своей иерархией, системой найма, обучения, мотивации и отпусками. Росту индустрии так же способствует развтие партнерских программ. Разработчики вредоносного кода продают или сдают в аренду продукт своим партнерам для дальнейшего взлома сети и развертывания программ-вымогателей.

Рост продаж доступов к взломанным корпоративным сетям

Рост спроса на рынке продажи доступов в скомпрометированные сети компаний подпитывает индустрию вымогателей с новой силой. За анализируемый в отчете период рынок продавцов доступов в даркнете вырос более чем в два раза, при этом средняя цена доступа уменьшилась вдвое по сравнению с аналогичным периодом ранее. Чаще всего злоумышленники реализуют свой «товар» в виде доступов к VPN и RDP (протокол удаленного рабочего стола).

Данные стилеров станут главным источником доступов в компании

Слитеры – вредоносные программы для кражи данных с зараженных компьютеров и смартфонов пользователей
В 2022 году данные, украденные с помощью слитеров вошли в топ-3 самых продаваемых «товаров» даркнета.

Увеличение количества утечек баз данных

97 жертв киберпреступлений в час означает, что жертва данного вида киберпреступлений появляется каждые 37 секунд.

82% успешных атак связаны с человеческим фактором, социальная инженерия по-прежнему в действии.

Киберпреступность затрагивает всех, не только бизнес.

Принято считать, что наименее уязвимы пользователей в группе до 20 лет. Однако, это не так, отчет компании Boston Consulting Group показывает, что 93% детей в возрасте от 8 до 17 лет пользуются Интернетом. Примечательно, что почти трое из четырех респондентов заявили, что столкнулись хотя бы с одной киберугрозой.

Количество киберпреступлений против детей увеличилось на 144% в 2020 году и продолжает расти на 5-9% в год.

Каждый второй ребенок в интернете сталкивается с кибербуллингом. Каждый третий с фишингом. Но на этом киберриски для детей не заканчиваются.

Аналитический центр MINDSMITH выделяет 23 вида существующих киберрисков для детей и подростков, каждый из которых представляет угрозу для эмоционального, психического, физического или финансового благополучия ребенка и 10 рисков и угроз будущего.

Существующие риски и угрозы

Криминализация, втягивание в криминальные практики

1. Вовлечение детей в криминальные сообщества
2. Продажа запрещенных товаров и услуг
3. Радикализация и экстремизм
4. Траффикинг

Маркетинговое давление, рискованные денежные отношения

5. Интернет как канал сбыта товаров, опасных для жизни и здоровья детей
6. Продвинутые методики маркетинга
7. Темные паттерны
8. Онлайн-мошенничество

Личностная атака, направленные против ребенка деструктивные действия

9. Кибербуллинг
10. Сталкинг
11. Груминг
12. Сексуальные домогательства

Цифровая эксплуатация, использование ребенка для создания цифрового Контента

13. Доксинг
14. Создание и распространение материалов с детской порнографией
15. Кража, сбор и эксплуатация персональных данных
16. Шерентинг

Информационное давление, информация, не предназначенная для детей и Подростков

17. Контент, содержащий сцены насилия
18. Порнографический контент
19. Дезинформация
20. Опасные тренды и челленджи

Аддикция, формирование зависимости от интернет-среды

21. Алгоритмы удержания внимания
22. Игровая зависимость
23. Избыточное использование интернета

10киберрисков и угроз будущего

1. Инфлюенсеры, рост их влияния и виртуализация

С ролью лидеров мнений, инфлюенсеров нельзя не считаться — они влияют на мнение и выбор людей, транслируют свои ценности и пользуются доверием со стороны аудитории. Инфлюенсеры также популярны и среди детей, которые формируют с ними парасоциальные отношения. При этом они не всегда осознают ответственность за идеи и мысли, которые транслируют своей аудитории

2.Взаимодействия между взрослыми и детьми в VR и метавселенных

В современных VR-приложениях степень контроля за взаимодействием детей и взрослых низка. Взрослые могут использовать аватары детей, а дети могут использовать аватары взрослых. же сейчас в VR существуют прецеденты кибербуллинга, сексуальных домогательств и других действий, которые способны распространить сопутствующие риски на детей и подростков

3. ИИ как инструмент преступников

Развитие технологий для производства дипфейков продолжится, и уже сейчас есть примеры систем, способных копировать лицо, голос и мимику, — это может использоваться мошенниками для обхода систем, базирующихся на биометрической верификации. И эти же технологии позволяют агрессивно настроенному ребенку создать фото или видео, в которых сверстник находится в компрометирующей ситуации.

4. ИИ как часть процесса воспитания

Дети впитывают информацию из окружающей среды и адаптируют ролевые модели взрослых, в том числе образ мышления. Образ мышления человека и аналогичные процессы у ИИ сильно отличаются. Когда дети начинают пользоваться голосовыми помощниками и умными устройствами с голосовым управлением в самом детстве, они могут неправильно понимать роль ИИ в их жизни.

5. Дистанционные способы эксплуатации детей

Одна из механик Web 2.0 — создание контента пользователями. Школьники уже сейчас абсолютно бесплатно производят контент на платформах коммерческих компаний. Например, сотни часов групповой работы уходят на проекты в видеоигре Roblox, прибыль за которые получает компания, а не фактические создатели контента. TikTok также очень популярен у детей и работает исключительно благодаря контенту, созданному пользователями.

6. Цифровой след и биометрические данные

Цифровой след начинает накапливаться ребенком с самого раннего возраста. Это является вектором для разнообразных атак

7. Трансформация социальных навыков детей

Длительный карантин погрузил людей в массовую изоляцию. Дети также стали жертвой обстоятельств — они начали больше общаться онлайн, пользоваться домашними устройствами с ИИ и формировать парасоциальные связи с блогерами и инфлюенсерами. Процесс освоения социального поля изменился, и дети, которые сильнее полагаются на интернет, могут иметь проблемы с традиционной формой социализации

8. Популяризация «серых» взаимодействий

Массовые ограничения доступа к ресурсам в интернете и возможная регионализация интернета уже привели к распространению различных сервисов и подходов по преодолению вводимых запретов. Такие программы популярны и у взрослых, и у детей, имеют удобный интерфейс и часто выкладываются в интернет с руководствами по настройке.
Популяризация «серых» взаимодействий может привести ребенка не только к изучению информационных и коммуникационных технологий, но и к вступлению в хакерскую ячейку на роль так называемого script kiddie — юного подмастерья более опытных хакеров.

9. Ужесточение информационной войны

Дети страдают не только от блокировок, будь то со стороны корпораций или правоохранительных органов — они нередко принимают раскрученные нарративы на веру. В результате они могут менять свои собственные позиции и проявлять активность — поддерживать свою сторону, занимать посты модераторов, создавать собственные сообщества. В контексте информационной войны все эти действия ставят детей на сторону баррикад. Но обратная сторона баррикад никогда не пуста. Санкции, применяемые к ребенку неформальными сообществами, государствами и корпорациями, не делают скидки на возраст и дальновидность ребенка

10. Рост цифрового разрыва

Цифровое неравенство и фактическое поражение детей из отдельных стран в гражданских правах может ограничить детей в способности получить своевременную помощь, провайдеры услуг не смогут воспользоваться полным спектром мер по противодействию рискам, угрожающим детям и подросткам, а правоохранительные органы будут ограничены в инструментах расследования преступлений. Дети рискуют остаться в менее благополучном, и следовательно, более опасном обществе, в котором сложнее найти помощь, а технологические меры будут развиваться медленнее, чем подходы преступников