Тенденции будущего. Преступления

Безмалый В.Ф.

Microsoft Security Trusted Advisor

Каждый раз в начале года эксперты в различных областях пытаются дать свои прогнозы: а что же нам готовит следующий день? Чаще всего эти прогнозы не сбываются или сбываются совсем иначе. Решил и я попробовать себя в нелёгкой роли прогнозиста. Сегодня мы с вами поговорим о том, а всегда ли новые технологии готовят нам только благо? В статье речь пойдёт о новых, вполне возможных, если не сегодня, то завтра, преступлениях, основанных на технологиях, уже существующих сейчас. Ведь не секрет, что первыми новые технологии осваивают военные и преступники.

С появлением новых технологий всё чаще появляются и новые преступления. Ещё не так давно мы с вами даже представить не могли, что потребуется специальное законодательство в области защиты персональных данных. Более того, прибыль интернет-злоумышленников сегодня намного превышает доходы офлайн злоумышленников. Но преступления в будущем потребуют ещё более высокого уровня сложности. По мере развития технологий мир взрывается вокруг нас.

Это уже происходит в области киберпреступности, но вскоре новые технологии освоят практически каждый уровень «традиционной» организованной преступности, включая всё: от дизайнерских наркотиков до обхода законов об иммиграции и крупномасштабной подделки торговых марок. Давайте попробуем заглянуть в страшное завтра и рассмотрим ряд будущих преступлений и новых технологий, которые будут использоваться для их выполнения.

Будущие преступления, которых сегодня ещё нет. Что день грядущий нам готовит?

В будущем с преступными целями будет использоваться 3D-печать для создания собственных пистолетов, не обнаруживаемых сегодняшними металлодетекторами, и, например, беспилотников. Вы мне возразите: создание 3D-печатного оружия — уже реальность. Да. Всё верно. Это уже реальность. К счастью, пока не массовая. Пока!

Все чаще будут использоваться глушилки мобильной связи, шпионское ПО, оборудование для генной инженерии. Практически каждая новая технология, создаваемая с лучшими намерениями, в будущем может и будет использоваться против нас. Ведь заказчиками чаще всего выступают военные, силовые структуры и преступность!

Достаточно сказать, что преступные умы непрерывно работают, чтобы сфабриковать новые возможности использования каждой из этих новых областей.

Преступления и беспилотники

Сегодня законы о применении беспилотников чаще всего находятся в стадии разработки. Вот те области преступлений, в которых беспилотники будут использоваться в ближайшем будущем:

1. **Перевозка незаконных веществ** — бомбы, яды, наркотики, человеческие органы и т. д.
2. **Оружие** — оборудование дронов пушками, пулемётами, лазерами, тазерами, огнемётами и многим другим.
3. **Вуайеризм** — шпионаж за людьми в их резиденциях или в пределах личного пространства.
4. **Подрывной маркетинг —** приёмы, которые удивляют и буквально переворачивают с ног на голову наше сознание. Он достигает одной, самой главной цели: товар или торговая марка надолго врезается в память, потому что делает что-то не так, как все.

5. **Незаконная стрельба или уничтожение беспилотных летательных аппаратов.** Число обладателей анти-дрон оружия растёт непрерывно. Более того, если несколько лет назад появление такого оружия считалось чем-то из области фантастики, то сегодня это реальность. Дрессированные хищники, направленные ручные глушилки, стационарные системы для перехвата управления (пока военные, но ведь всё было пока…).
6. **Шум.** Будущие беспилотники с динамиками и прикреплёнными системами звукоусиления (думаю, летающие концертные акустические системы) могут быть превращены в разрушительное оружие. Вспомните опыты с инфразвуком. А если учесть возможность миниатюризации?
7. **Летающие фальшивые мобильные станции** для перехвата или глушения мобильных разговоров. Не так давно подобные станции, правда размещённые на небольших самолётах (вертолётах), применяла полиция Калифорнии. Кто следующий?
8. **Drone издевательства** — акты запугивания, угрозы или отображение постыдных фотографий.
9. **Дроны-истребители других беспилотных летательных аппаратов** — дроны, специально предназначенные для захвата или уничтожения других беспилотных летательных аппаратов.

Смешанная реальность

Представьте смешанную реальность. Игры, показывающие мир, в котором мы живём, только с визуальными накладками, которые делают людей вокруг нас невольными игроками и пешками. Нет такого? Разве? Вспомните Pokemon Go.

10. **Сбор толпы для совершения теракта.** Запускаем игру (тот же Pokemon Go) и собираем игроков в заранее определённом месте. Затем взрыв. На массовых мероприятиях место заранее проверяется полицией, проверяются и приходящие люди. В данном случае никто никого не проверяет. Да и люди приходят туда абсолютно произвольно — в ходе игры.
11. **Смешение реальности и игры, предназначенное для набора баллов путём нанесения различных повреждений другим игрокам.** Пользователи набирают очки, нанося физические ушибы, словесные оскорбления, используя публичные осуждения и даже физическое отключение или убийство.
12. **Целенаправленное искажение реальности для получения выгоды за счёт других.**

История. Атаки на подмену памяти о прошлом.

Мы сегодня всё чаще и чаще видим подобное. Пока с помощью телевидения, фильмов, атак через интернет. Что можем этому противопоставить? Практически ничего. Народ ищет зрелища!

13. **Наглый обман и перевирание прошлого.** Сбор фрагментов из жизни человека может заставить выглядеть его дураком. Мы все имеем свои скелеты в шкафу. У всех бывают ошибки, и здравый смысл отказывает нам в тот или иной момент.
14. **Явный ревизионизм.** Для некоторых создание ложной реальности, ложных выводов и переосмысление событий прошлого станет новой формой уголовного искусства. Вспомните сегодняшние заявления в некоторых изданиях, что концлагерь Освенцим (Аушвиц) освобождала американская армия. А ведь этому уже верят!
15. **Ложные мемы** — продолжатели ложных исследований и опросов. Здесь тоже можно привести массу примеров ложных исследований. Вспомните заявление США о наличии в Ираке оружия массового поражения. Оружие не нашли, но страна разгромлена. Можно вспоминать и вспоминать.
16. **Поддельные выводы** — изобразительное искусство достижения ложных выводов.

Социальные шантажисты

Во многом таким же образом, как персонализированная система маркетинга компании Google обеспечивает целевую рекламу, запугивание может быть создано с единственной целью — доставка высокорелевантных угроз. Как только обостряется киберпреступность, мы рискуем иметь наши социальные структуры перерождающимися в невидимые сообщества мафиозного типа шантажистов. В то время как большинство из них будет делать это за деньги, другие — из-за мести, немногие, если таковые найдутся, будут способны понять происходящие истинные закулисные разборки.

17. **Шантаж путём угрозы детям**. С социальными медиа всё чаще будет легко запугать угрозой причинения вреда ребёнку, другу или любимому человеку. Тем более что дети и наши пожилые родственники атакуются гораздо проще. Вспомните телефонные звонки: «Ваш сын попал в милицию…»
18. **Угроза изоляции.** Мы все по своей природе социальные существа и угроза отчуждения (и тем самым изоляции нас от друзей) может быть хуже смерти.

Угрозы ИИ

Очень легко будет полагаться на искусственный интеллект, который будет помогать нам принимать многие решения: куда идти, с кем встретиться, какую музыку слушать и даже как развлечь наших детей. Но что происходит, когда наш ИИ используется злоумышленниками?

19. **Дорожно-транспортные происшествия.** Так как умные автомобили без водителя и беспилотные летательные аппараты будут управляться ИИ, то программное обеспечение, скомпрометированное злоумышленниками, может нарушить всю транспортную сетку через ряд аварий, несчастных случаев и массовых пробок. Вспомните опыт, в ходе которого автомобиль с ИИ заставили свернуть с дороги, просто нарисовав неверную дорожную разметку. А сколько таких ошибок возможны ещё?
20. **Потеря данных** — потеря информации, изменения и целенаправленные искажения информации.
21. **Отключение электропитания, других коммунальных услуг —** отрезать некоторые компании или людей от коммунальных услуг и другой помощи, в которых они нуждаются. Уже сегодня это реальность, достаточно вспомнить массовое отключение электроэнергии в США или нечто подобное на Украине, произошедшие в результате вирусной атаки.
22. **Паралич линий связи.** ИИ скоро станет важной частью наших повседневных процессов принятия решений, но перезагрузка ИИ, эквивалентная «отказу в обслуживании» вызовет огромные проблемы.

Пересмотр прошлого

Мало что в жизни более тревожно, чем уничтожение наследия людей после смерти. Увы, но изменить память проще, фактически убив мёртвых и начав перевоспитывать детей, которые в данном случае являются первичными субъектами этого вида атак. Мы уже сегодня наблюдаем это на примере вопросов о второй мировой войне, где уже основными победителями называются армии США и Великобритании.

23. **Ложные мотивы, ложные намерения.** Если человека уже нет в живых, чтобы он мог оправдать свои действия, то относительно просто исказить его мотивацию. Все чаще так происходит с прошлым. Пока историческим прошлым, но ведь это пока!..
24. **Последствия выдуманных поражений.** Наш круг тесно связан с друзьями и знакомыми. Этот круг расширяется в геометрической прогрессии, так что его относительно легко взломать. В данном случае взламывать будут не вас, а ваших друзей. Но вам-то от этого вряд ли будет легче.

25. **Изменение мышления.** Изменяющиеся причинно-следственные связи стали обычным инструментом, используемым в политических кругах, чтобы изменить мышление людей, заставить их сделать неправильный вывод. Примеров здесь, уверен, можно привести массу. Причём вы это сделаете, может быть, даже лучше меня.
26. **Переписывание выводов, используя неверные оценки воздействия.** Большинство злоумышленников (и не только они) имеют большой набор инструментов, в том числе и способности превратить любое, самое маленькое событие в жизни в гигантское, весьма важное, переврав при этом само событие. Примеров тоже можно привести массу. Вспомните атаки химического оружия в Сирии. Было или не было — доказать сложно, но вот нагнать страху…
27. **Возможность вогнать финансовые системы стран в каменный век.** Сегодня, а тем более завтра это сделать будет куда проще.
28. **Пандемии.** Смертельные инфекции и вирусные заражения будут появляться гораздо чаще и быстрее, чем когда-либо, в изготовлении, распространении и заражении в течение ближайших десятилетий. Думаю, что биологическое оружие никто не отменяет, увы. Пример того, что может произойти, у нас перед глазами.
29. **Паралич из-за отключений связи.** Так как мы стали больше полагаться на данные связи, голосовые сообщения, то наши ключевые точки уязвимости становятся всё более очевидными.
30. **Один тщательно направленный взрыв может вызвать неизмеримый ущерб,** причём это может быть как реальный, так и информационный взрыв.

Преступления руками роботов

С помощью растущего дисбаланса между супербогатыми и супербедными вероятным сценарием будет расширение масштабов техно-стелс войны подпольного типа с технологиями хакеров, используемыми для разрушения наших систем, промышленности и правительства новыми и необычными способами.

31. **Беспилотники, роботы, беспилотные автомобили и манипуляторы данных злоумышленников.** Увы, это скоро станет общей частью словаря каждого будущего преступника. Уже сегодня известно о смерти человека от «рук» робота. Неверное, программирование. А где гарантии, что это не случится специально?
32. **Атаки на медицинские системы.** Атака на инсулиновые помпы, на прочее медицинское оборудование, результатом которых стала смерть пациента. Это сегодня. А завтра?
33. **Управление психо-ботами.** Один слегка ненормальный психо-бот может быть в тысячу раз более разрушительным, чем один террорист-смертник сегодня.

Криптовалюта

Криптовалюты стали идеальным инструментом для сокрытия сделок.

34. **Тайные операции.** Криптовалюты открывают дверь для действительно секретных коммуникаций и денежных переводов.
35. **Хранение богатства с помощью криптовалют** становится невозможным для сдерживания преступной деятельности, нет никакого способа, чтобы понять, как делаются операции и как эти деньги хранятся.

Генная инженерия

Генная инженерия уже давно обещала препараты для лечения заболеваний и общего улучшения состояния человека. В то же время манипуляция генами представляет собой инструмент, который может быть использован в преступных целях.

36. **Создание деструктивных новых форм жизни.** Мы не имеем ни малейшего представления о том, какие вредные новые формы жизни могут быть и будут созданы. Где гарантия, что в этот момент не создаются новые штаммы вирусов? Их нет!
37. **Создание суперзаразных новых болезней** будет включать в себя всё, что ставит под угрозу здоровье, безопасность или жизнеспособность людей.
38. **«Редактирование» человека.** Без сдержек и противовесов учёные могут попытаться реализовать рискованные схемы мутации человека. Уже сегодня в Китае созданы два ребёнка с искусственно подправленными генами. А что будет завтра?
39. **Создание суперребёнка.** Люди, желающие сделать себе имя, могут проверить экстремальные теории проектирования младенцев.

Взлом мозга человека

Нам нравится думать о собственном мозге, как о безопасном убежище для наших мыслей, но что, если это не так? Что произойдёт, когда наше серое вещество постараются взломать?

40. **Имплантация ложных воспоминаний.** Понимание человеческого мозга улучшится, при этом возможен взлом воспоминаний или вызов провалов в памяти. Это может стать обычным явлением.
41. **Слитые воспоминания.** Без нашего ведома мозг может быть взломан, а воспоминания «слиты» на другой носитель.
42. **Использование ложных директив вытеснит свободную волю.** Мы высоко ценим свободу воли. А так ли уж она свободна? Мы можем быть вынуждены совершать преступления, даже если физически сопротивляемся. Увы, под воздействием определённых препаратов и гипноза это возможно уже сегодня.
43. **Внедрение доминирующих личностей.** Для властных преступников вложенная доминирующая личность будет отклонять возражения пассивной личности и заставит её соответствовать.

Время преступления

44. **Временные законы.** Напрасно тратить наше время скоро станет преступлением.
45. **Штрафы за потерянное время.** Поскольку время является дефицитным товаром, мы скоро увидим штрафы за потерянное время.

Террористы и умные транспортные средства

Впереди нас ожидает небольшая потребность в смертниках, так как взлом умных транспортных средств откроет дверь в совершенно новый набор опасностей.

46. **Фанатики.** Умные транспортные средства, оснащённые бомбами, перевозящие опасных животных, химическое оружие, боевые отравляющие вещества и т. д.
47. **Похищение детей/похищение людей:** друзей, родственников, детей, путешествующих без сопровождения из школы или после школы.
48. **Глушение связи.** Глушилки связи будущего могут быть практически необнаруживаемы с их способностью блокировать все формы света, тепла, звука.
49. **Самоуничтожающиеся генераторы страха.** Мобильные наземные мины, предназначенные для запугивания людей.

Мегапроект манипуляторы

50. **Ложные утверждения о рабочих местах.** Большинство стран будут активно вкладываться в соответствие их использования людьми, так что большинство предложений будут приходить с фиктивными претензиями на работу.

51. **Обманчивые экономические выгоды.** Претензии крупномасштабной экономической выгоды всегда привлекательны для политиков, но благие намерения не делают жизнеспособными бизнес-операции.
52. **Придуманные потребности.** Инфраструктуру, как правило, легко продать, особенно если существующая не устраивает, но жулики будут эксплуатировать гигантский проект фиктивной «потребности».
53. **Фиктивный учёт.** Мир мегапроектов всё чаще будет притягивать злоумышленников.

Промышленный геноцид

54. **Манипулирование глобальным спросом.** Когда покупатели вынуждены уйти, отрасль просто перестанет существовать.
55. **Прекращение финансовой поддержки** — финансисты могут манипулировать, отступая от сделки.
56. **Манипуляция частями или материалами, вызывающая резкий рост расходов.** Наиболее успешные продукты образуются вокруг важных компонентов, которые часто трудно сделать и трудно получить. Умышленное создание нехватки может стать преградой в цепочке поставок завода-изготовителя.
57. **Причинение вреда с помощью слухов.** Хорошо разработанная дезинформация, направленная на создание разнообразных слухов, может легко заставить упасть даже лучшие акции. В будущем этот процесс не займёт много времени, чтобы заставить акции падать всё ниже и ниже.

Проблемы, которые находятся за пределами наших возможностей

Увы, с каждым годом DarkNet становится всё «темнее».

58. **Уничтожение экономики целой страны.** Это уже происходит на определённых уровнях. С помощью нескольких новых инструментов это будет только легче и быстрее.
59. **Массовые стихийные бедствия.** В будущем наша способность контролировать ураганы, землетрясения, град или саранчу будет в пределах досягаемости.
60. **Принуждение АЭС к саморазрушению.** Каждая новая технология даёт злоумышленникам дополнительные возможности.

Заключение

Как ни странно, в будущем преступления станут всё более и более изощрёнными. С одной стороны, человек получает всё больше и больше власти, с другой – гонка вооружений в области ИТ толкает преступность на новый уровень.

С одной стороны, хорошо, если удаётся поймать злоумышленников, с другой — плохо, ведь правительство постоянно заглядывает нам через плечо.

Бизнес-модель «преступление-как-сервис» будет развиваться в сложные бизнес-операции буквально с тысячами невольных людей, занимающихся на разных уровнях, но мало кто будет знать точный характер плана.