чительной компетенцией соответствующих государственных органов. При этом они полагают, что и финансовые издержки на создание системы обеспечения безопасности КВО должно нести государство. Одновременно администрация (собственники) КВО в ряде случаев заинтересованы в сокрытии фактов инцидентов безопасности на объектах, так как предание их гласности может повлечь за собой привлечение виновных лиц из числа владельцев (собственников) КВО, его руководства и иных работников объекта к уголовной, административной или иным установленным видам ответственности, а также значительные расходы на устранение причин и условий их возникновения.

Создание и поддержание системы обеспечения безопасности КВО требуют значительных финансовых ресурсов. Например, в 2004 г. хозяйствующие субъекты транспортной деятельности в РФ на обеспечение безопасности затратили собственных средств около 1,2 млрд р. (примерно 41 млн долл. США). Уже в 2011 г. только ОАО «РЖД» на цели обеспечения транспортной безопасности выделило 12,77 млрд р. (около 425 млн долл. США). При этом специалистами отмечается, что затраты на создание и поддержание систем обеспечения транспортной безопасности необходимо соизмерять с возможными рисками. Так, в результате взрыва в зале международных прилетов московского аэропорта Домодедово 24 января 2011 г. погибли 37 человек и 159 причинен различной степени тяжести вред здоровью, материальный ущерб составил 40 520 928 р. (примерно 1,35 млн долл. США). Между тем планируемые в 2014 г. затраты ОАО «Авиационная компания «Трансаэро» составили бы 22 млрд 720 млн р. (примерно 570 млн долл. США), а в государственном унитарном предприятии Москвы «Московский ордена Ленина и ордена Трудового Красного Знамени метрополитен имени В.И. Ленина» – 24,357 млрд р. (примерно 600 млн долл. США).

В настоящее время установлен целый ряд требований и правил в области обеспечения безопасности КВО. Вместе с тем не предусмотрена ответственность за неправомерное вмешательство в деятельность КВО и нарушения в области обеспечения безопасности КВО. Фактически отсутствуют организационно-правовые механизмы, обеспечивающие пресечение актов незаконного вмешательства в функционирование КВО, а также за принудительное выполнение администрацией (собственниками) КВО соответствующих требований и правил.

В целях преодоления указанных и иных проблем в сфере обеспечения безопасности КВО на современном этапе представляется целесообразным:

рассмотреть вопрос о принятии законодательного акта в сфере безопасности КВО;

внести изменения и дополнения в Уголовный кодекс Республики Беларусь и Кодекс Республики Беларусь об административных правонарушениях в части, касающейся установления соответствующих видов ответственности за неправомерное вмешательство в деятельность КВО, а также за нарушения в области обеспечения безопасности КВО;

дальнейшее развитие системы обеспечения безопасности КВО осуществлять с использованием в том числе механизмов государственно-частного партнерства.

УДК 343.3

В.И. Пикта

СОДЕРЖАНИЕ ИСПОЛЬЗОВАНИЯ ПРОГРАММ-ВЫМОГАТЕЛЕЙ КАК УСЛУГИ

В последние годы стремительно расширяется инструментарий киберпреступников, что позволяет даже тем, кто не обладает техническими знаниями, проводить атаки на информационные системы с использованием различного вредоносного программного обеспечения. Одним из новейших способов совершения киберпреступлений является использование программ-вымогателей как услуги (RaaS – Ransomware as a Service). Защита от данного вида преступления очень важна, поскольку использование программ-вымогателей как услуги может повлечь за собой значительные последствия для физических лиц и организаций. Атаки RaaS могут привести к шифрованию конфиденциальных данных и потере доступа к важным системам, что ведет к значительным сбоям в работе информационных систем и финансовым потерям.

Для организаций атака RaaS может привести к потере доходов, подрыву репутации и долгосрочным финансовым потерям. В некоторых случаях организации могут быть вынуждены заплатить выкуп, чтобы восстановить доступ к своим данным, что только сильнее побуждает организаторов к совершению еще большего количества аналогичных преступлений ввиду их высокой эффективности. Кроме того, атаки RaaS могут повлечь за собой проблемы соблюдения требований нормативных правовых актов, поскольку от организаций может потребоваться сообщить государственным органам о компрометации персональных данных.

Для физических лиц RaaS-атака может привести к потере личной информации и финансовым потерям. В некоторых случаях злоумышленники могут потребовать от жертв оплату за восстановление доступа к их личным файлам.

Программа-вымогатель как услуга (RaaS) – это преступная бизнес-модель, в которой киберпреступники предлагают свои инструменты и услуги другим лицам или группам обычно за процент от суммы выкупа. Поставщики программ-вымогателей обычно предлагают ряд услуг, включая предоставление вредоносного кода программы, хостинг веб-сайта для оплаты выкупа и поддержку клиентов, осуществляющих атаки.

Программа-вымогатель является типом вредоносных программ, которые шифруют файлы жертвы и требуют выкуп в обмен на ключ для расшифровки. Обычно данная разновидность вредоносных программ распространяется через фишинговые письма или путем использования уязвимостей в программном обеспечении.

Одной из основных проблем при выявлении и раскрытии преступлений, связанных с использованием программ-вымогателей как услуги, является идентификация лиц или групп, стоящих за такими атаками. Поставщики данной услуги часто используют анонимные способы оплаты и сложную сетевую инфраструктуру, чтобы скрыть свою личность. Кроме того,

использование шифрования и других инструментов для сокрытия от обнаружения затрудняет отслеживание злоумышленников правоохранительными органами.

Одним из основных направлений совершенствования тактики борьбы с программами-вымогателями как услугами является исследование методов и приемов, которые правоохранительные органы используют для расследования и пресечения деятельности указанных сервисов. Это может включать в себя изучение правоприменительной практики по расследованию данной категории дел, международного опыта в выявлении подобных преступлений, а также изучение инструментов и технологий, которые используются для отслеживания и обнаружения RaaS-групп. Кроме того, может быть полезно изучить психологию и мотивацию операторов RaaS, а также тактику, которую они используют, чтобы избежать обнаружения. Также важно быть в курсе последних тенденций и событий в сфере RaaS, поскольку тактика и инструменты, используемые RaaS-группами, постоянно совершенствуются.

Для защиты от атак с использованием RaaS организациям следует обеспечить регулярное исправление и обновление своих сетей и систем, чтобы предотвратить использование уязвимостей. Они также должны доводить до сотрудников информацию об опасности фишинговых писем и других распространенных методов атак. Кроме того, наличие надежного плана резервного копирования и аварийного восстановления может помочь организациям быстро и эффективно восстановиться после атаки программы-вымогателя.

В заключение следует отметить, что программа-вымогатель как услуга (RaaS) – это прогрессирующая тенденция в киберпреступности, позволяющая даже тем, кто не обладает техническими навыками, проводить разрушительные атаки на информационные системы. Организациям важно принять меры по защите от таких атак и быть готовыми к быстрому и эффективному восстановлению в случае, если они стали жертвой атаки RaaS. Правоохранительным органам необходимо основное усилие направить на совершенствование профилактической базы для эффективного предупреждения RaaS-атак, а также разработать научно-методические и научно-практические рекомендации по грамотному и эффективному раскрытию и расследованию атак с использованием программ-вымогателей.

УДК 351.74

С.В. Пилюшин

КОНТЕНТ-АНАЛИЗ В АНАЛИТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

Эффективность аналитической деятельности любого правоохранительного органа во многом определяется уровнем организации информационно-аналитического обеспечения. Наличие достаточного количества объективной информации, а также современных средств ее обработки не только позволяет осуществлять анализ и принимать на основе его результатов оптимальные управленческие решения, но и способствует совершенствованию методов работы, приемов и способов его проведения.

Вся аналитическая деятельность выстраивается на основе информации, получаемой из различных источников. Умение ее обобщать, анализировать, подмечать и выделять из потока разобщенных сведений самое существенное, главное, синтезируя новые, ранее не известные сведения, делает эту деятельность плодотворной, а специалиста квалифицированным.

Как правило, содержание источников – носителей информации, представляющей интерес для правоохранительных органов, может быть наполнено достаточно большими объемами данных, из общего потока которых еще только предстоит выделить значимую информацию, которая в дальнейшем будет использована в решении различных задач.

Эффективным для более детального изучения их содержания видится применение метода контент-анализа – формализованного аналитического метода исследования первичных материалов, позволяющего выявлять и измерять в их содержании получившие свое отражение характеристики социальных явлений.

Более широко понять содержательную сторону контент-анализа и эффективность его применения в аналитической деятельности возможно, обратившись к его истории. Еще на пороге XX в. контент-анализ применялся для объективного, систематического и квантитативного описания явно выраженного содержания коммуникации. Однако позднее концептуальные представления о его содержании изменились, сместив акцент в плоскость раскрытия латентного содержания сообщений через изучение реальных данных источника информации.

Независимо от того, какие именно носители информации (материалы) исследуются, будь то письменные или электронные тексты, фото-, видео- или аудиофайлы, метаданные этих файлов, в научной литературе основные преимущества метода контент-анализа связывают с его оперативностью, незатратностью, легкой воспроизводимостью, что в целом позволяет получать из массивов разрозненных данных выводное знание.

Ряд ученых отмечают, что тексты, представляя собой сложный феномен, выполняют функции коммуникации, хранения и передачи информации, отражения жизни индивида, определенного исторического периода и социальных явлений. Проводя их контент-анализ, представляется возможным установить присутствие в них ключевых слов, зафиксировать смысловые единицы содержания, частоту их употребления и т. д.

Однако в отличие от текстовых сообщений, когда их содержание часто может быть достаточно очевидным, звуковые и изобразительные (фото-, видео-) материалы в терминах семиотики представляют собой прямое незакодированное сообщение, содержанием которого является отображаемая реальность. Такие материалы, выступая в качестве инструмента познания, в определенных случаях могут скрывать отдельный зафиксированный реальный фрагмент действительности.

Раскрытие латентного содержания в таких материалах, которые могут быть получены, например, в ходе проведения поисковых и оперативно-розыскных мероприятий, производства следственных действий, сопоставимо с распознанием при-