ции и изменения обстановки в зависимости от огромного множества факторов, а также отсутствие возможности ее глобального отслеживания в режиме реального времени не позволяет эффективно принимать меры контроля оперативной обстановки на обслуживаемой территории. При этом при проведении анализа оперативной обстановки не всегда в полной мере возможно охватить все факторы ее формирования и изменения. Часто не учитываются социальные процессы в обществе, современные тенденции и экономическое состояние определенной территории. Технология «Большие данные», в зависимости от ее реализации, способна в режиме реального времени собирать и анализировать информацию о текущей обстановке на территории обслуживания органа внутренних дел и подготавливать оперативные прогнозы изменения криминогенной обстановки.

Таким образом, основным преимуществом использования рассматриваемой технологии в правоохранительной деятельности является формирование оперативного прогнозирования, способного оказать помощь сотрудникам органов внутренних дел в реагировании на формирующиеся изменения, касающиеся предупреждения, выявления и пресечения преступлений.

УДК 343.3

В.И. Пикта

НЕКОТОРЫЕ АСПЕКТЫ РАСПРОСТРАНЕНИЯ ПРОГРАММ-ВЫМОГАТЕЛЕЙ

Обеспечение защищенности информационных систем является одним из самых важных аспектов обеспечения информационной и национальной безопасности. Информация, в нынешних реалиях, является самым ценным объектом, который требует особого режима защиты. В таких условиях широкое распространение информации как ресурса послужило появлению вредоносного программного обеспечения, основной целью которого является компрометация информации и информационных систем.

Вредоносное программное обеспечение – это любое программное обеспечение, которое негативным образом влияет на работу персонального компьютера или радиоэлектронного устройства. Вредоносное программное обеспечение может быть представлено в виде всплывающего окна, которое не позволяет пользователю получить доступ к основному функционалу интернет-ресурса или к программному обеспечению, копирующему финансовую информацию с компьютера жертвы.

Согласно исследованиям «Лаборатории Касперского» в последние годы число новых семейств и разновидностей вредоносного программного обеспечения стремительно растет. «Лаборатория Касперского» ежедневно выявляет около 325 000 уникальных образцов вредоносных программ. Под угрозой находятся как домашние пользователи, так и крупные компании, банки, критическая инфраструктура, государственные организации, промышленные предприятия, использующие автоматизированные системы управления технологическими процессами.

Среди огромного ландшафта угроз в сфере распространения вредоносного программного обеспечения одним из лидеров выступают программы-вымогатели (шифровальщики). Данная угроза свойственна всем сферам функционирования информационных систем государственного и частного сектора. По статистическим сведениям, за 2021 г. мировой ущерб от распространения программ-вымогателей составляет около 20 млрд долл. США в связи с выплатой выкупов вымогателям и простоями.

Программа-вымогатель (от англ. ransomware – компиляция слов ransom – выкуп и software – программное обеспечение) является разновидностью вредоносного программного обеспечения, предназначенного для блокирования доступа к компьютерным системам или предотвращения считывания компьютерной информации (преимущественно с использованием методов шифрования), после чего от жертвы за дешифрование информации требуется выплатить денежные средства.

В научной литературе программы-вымогатели определяются как тип вредоносного программного обеспечения, которое поражает компьютерные системы, ограничивая доступ пользователей к данным, хранящимся в скомпрометированных системах. Восстановление измененной информации является трудоемким процессом, и многие жертвы выплачивают выкуп в целях получения ключей дешифрования. Однако выплата выкупа не гарантирует, что файлы будут дешифрованы или программа-вымогатель будет отключена или удалена для предотвращения повторения заражения информационных систем в будущем.

Угрозы, исходящие от программ-вымогателей, зависят от типа вируса, вследствие чего представляется возможным выделить две основные категории указанных программ: программы-блокировщики и программы-шифровальщики.

Программа-блокировщик – тип программ-вымогателей, предназначение которых блокировать работу персонального компьютера или мобильного устройства, с целью последующего требования выкупа. В отличие от программ-шифровальщиков, блокировщик не шифрует компьютерную информацию, а блокирует доступ к основному функционалу компьютерной системы. Предметом посягательства данного ви-

да программ-вымогателей может выступать как устройство в целом, так и отдельное программное обеспечение, например, веб-браузер.

Программа-шифровальщик – тип программ-вымогателей, которая модифицирует пользовательские данные, путем использования различных алгоритмов и техник шифрования. После кодирования информации вредоносное программное обеспечение инициирует подключение к удаленному рабочему столу и пересылает информацию об идентификаторе зашифрованного устройства, для последующего восстановления модифицированной компьютерной информации.

Указанные типы вредоносного программного обеспечения могут распространяться по следующим векторам: перенаправление трафика; вложения электронной почты; ботнеты.

Перенаправление трафика. Данный вектор является наиболее распространенным способом побудить пользователя перейти по ссылке на вредоносную рекламу или перенаправить веб-трафик пользователя на другой интернет-ресурс, на котором размещено вредоносное программное обеспечение в виде набора различных эксплоитов. Чаще всего это встречается на интернет-ресурсах с порнографическим содержимым, пользователя с указанных сайтов перенаправляют на портал, предлагающий бесплатные игры или обновления для пользовательских приложений. При загрузке указанного контента вредоносное программное обеспечение использует уязвимости устройства пользователя, что приводит к блокировке либо шифрованию пользовательской информации.

Вложения электронной почты. Электронные письма с вложениями или ссылками побуждают пользователей открывать и получать доступ к веб-ресурсам, содержащим программу-вымогатель. На первый взгляд жертве кажется, что электронное письмо отправлено подлинным корреспондентом, так как вложения могут содержать электронный счет за потребляемую электроэнергию, налоговую или юридическую документацию, или даже содержат информацию от лиц, ищущих работу с просьбой открыть вложение или перейти по ссылке, чтобы актуализировать информацию о пользователе.

Ботнеты. В последние годы особую популярность приобрел данный вид вредоносного программного обеспечения, так злоумышленники стремятся взять под контроль миллионы устройств по всему миру и таким образом управлять огромной сетью устройств, которые можно использовать для осуществления атак типа «отказ в обслуживании» (DDoS), тем самым блокируют доступ к информационным системам. Распространяется данный вид вредоносного программного обеспечения при помощи загрузчиков путем компрометации пользовательских компьютерных систем и сетей, после чего загружается вредоносное программное обеспечение в качестве второго шага. Загрузчики пред-

ставляют собой легальное программное обеспечение, такое как бесплатные игры и инструменты, которые не содержат вредоносного кода, а загружает его позже.

В данной ситуации для получения необходимой информации о распространителе вредоносного программного обеспечения важно проанализировать данные, хранящиеся в журналах обращений к сетевому оборудованию, либо оперативного взаимодействия с организациями, представляющими услуги в качестве хостинг- и интернет-провайдера.

Данный перечень угроз не является исчерпывающим. Преступность не ограничивается существующими решениями, а постоянно совершенствует инструменты для проведения кибератак с целью компрометации компьютерных систем и сетей.

Подводя итог изложенному, важно особо отметить необходимость в разработке научно-методических и научно-практических рекомендаций для сотрудников правоохранительных органов по грамотному и эффективному извлечению следов активности программ-вымогателей, и сохранению данных следов для последующего изучения и использования в суде в качестве доказательства.

УДК 343.985.8

С.В. Пилюшин

О НЕКОТОРЫХ ПРОБЛЕМАХ МЕТОДОЛОГИИ КАТЕГОРИАЛЬНО ПОНЯТИЙНОГО АППАРАТА АНАЛИТИКИ В СИСТЕМЕ ОПЕРАТИВНЫХ ПОДРАЗДЕЛЕНИЙ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Изменения, происшедшие за последние годы в социальной, экономической жизни общества, законодательстве, возникновение новых форм проявления преступности, в том числе основывающихся на использовании информационных технологий, оказывают существенное влияние на процессы принятия управленческих решений, постоянное усложнение которых объективно требует максимального включения в оперативно-розыскную практику современного аналитического инструментария, формирования и развития аналитических компетенций.

Очевидно, что в сложившихся условиях борьбы с преступностью назрела необходимость глубокого понимания и осмысления сущностного содержания аналитики как особого вида деятельности, обоснования используемой в процессе выявления и раскрытия преступлений ее определенной модели конкретными оперативными подразделениями.