ИССЛЕДОВАНИЕ ИНДИКАТОРОВ КОМПРОМЕТАЦИИ ДЛЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИОННЫХ И КИБЕРФИЗИЧЕСКИХ СИСТЕМ

Мещеряков Р.В.[1], Исхаков С.Ю.[2]

Цель работы: *исследование существующих стандартов индикаторов компрометации и методов обмена ими для обогащения систем защиты информационных и киберфизических систем.*

Метод исследования: *системный анализ открытых источников данных об индикаторах компрометации, стандартах их описания и методов обмена при организации кибербразведки.*

Полученный результат: *сформулированы актуальные проблемы проактивного поиска угроз на примере применения открытых источников индикаторов компрометации при обработке потоков событий в системах управления событиями безопасности. Предложена классификация индикаторов, получаемых из внутренних источников. Сформулированы основные проблемы обработки динамических потоков данных об угрозах в условиях изменяемых векторов атак.*

Установлено, что в отрасли кибербразведки в настоящее время отсутствует единое решение в части стандартизации обмена информацией между различными платформами, но при этом имеют место ряд доминирующих стандартов и форматов обмена подобными данными. В ходе подготовки обзора существующих стандартов рассмотрены и структурированы задачи выявления ранее неизвестных методов атак на основе применения открытых источников индикаторов компрометации при обработке данных в системах управления инцидентами безопасности и предложены методы их решения.

Научная новизна: *представленная статья является одной из первых отечественных работ, посвященных анализу актуальных исследований по организации работы с источниками данных кибербразведки. Рассмотрены и систематизированы источники индикаторов компрометации и предложена их классификация. Сформулированы основные проблемы обработки динамических потоков данных об угрозах в условиях изменяемых векторов атак.*

Ключевые слова: *индикатор компрометации, кибербразведка, контекст, киберфизическая система, система управления событиями безопасности, обогащение, ранжирование.*

DOI:10.21681/2311-3456-2022-5-82-99

Введение

Последние изменения в мировом сообществе и действительность современной информационной среды обуславливают ежедневно меняющийся ландшафт киберугроз, что особенно характерно для высокоавтоматизированных отраслей промышленности, таких как робототехника и киберфизические системы. Эффективное обнаружение и предотвращение атак на подобные инфраструктуры требует применения механизмов, позволяющих выявлять ранее неизвестные методы и тактики действия злоумышленников.

При этом одной из важнейших задач при обеспечении надлежащего уровня защищенности киберфизических систем является автоматизированный мониторинг событий информационной безопасности как центра управления, так и всей инфраструктуры. Целью такого мониторинга является своевременное оповещение и предупреждение об обнаруженных аномалиях в работе системы, прямо или косвенно являющихся свидетельством инцидента безопасности.

Один из основных вызовов современной картины мира заключается в сокращении времени реагирования на инциденты и получении актуальной картины угроз, поскольку вторжения в киберфизические системы производственных процессов, запущенных в кри-

1 Мещеряков Роман Валерьевич, доктор технических наук, профессор, главный научный сотрудник ИПУ РАН, Москва, Россия. E-mail: mrv@ieee.org, ORCID: 0000-0002-1129-8434

2 Исхаков Сергей Юнусович, кандидат технических наук, начальник отдела анализа и реагирования на компьютерные инциденты ПАО «Промсвязьбанк», Москва, Россия. E-mail: sergey@iskhakov.ru, ORCID: 0000-0003-3346-9262

тической инфраструктуре, недопустимы, что в свою очередь закреплено на законодательном уровне. В сфере информационной безопасности сегодня активно формируется тренд применения проактивного опережения действий злоумышленников с использованием методов кибербразведки. Среди причин подобных тенденций можно выделить, в первую очередь, ограниченность использования классической антивирусной защиты на базе сигнатур и эвристического анализа. Например, такие технологии не позволяют выявить бесфайловые атаки и несанкционированное применение легитимного программного обеспечения (ПО). Кроме того, количество внедряемых на объектах средств защиты информации (СЗИ) зачастую так велико, что генерируемые ими данные о возможных инцидентах сложно поддаются анализу. Одним из основных методов в решении данной задачи является использование индикаторов компрометации (indicator of compromise, IoC) [1] для обогащения СЗИ в информационных и киберфизических системах.

К числу отличительных особенностей большинства решений проактивного поиска угроз относится формирование наборов индикаторов, которые позволяли бы выявить ранее неизвестную атаку на ранних стадиях. Поскольку эффективность таких обнаружений сводится к реальной возможности реагировать на угрозу, то необходимо ранжировать подобные индикаторы в соответствии с их значимостью. Обсуждению данной проблемы и выдвижению собственных подходов и методов посвящено множество публикаций российских и зарубежных авторов, а также материалов докладов профильных конференций. Такая активность отражает заинтересованность мирового научного сообщества в создании комплексных решений в указанной области. Для оперативного получения подобных данных необходимо применение потоковой обработки индикаторов компрометации. Результаты исследований, рассмотренные далее, свидетельствуют о том, что в отрасли кибербразведки отсутствует единое решение в части стандартизации обмена информацией между различными платформами. Доминирующим является стандарт описания индикаторов STIX [2], при этом в зависимости от контекста в ряде случае его применение нецелесообразно.

В этой связи в статье представлен обзор стандартов описания индикаторов компрометации и форматов обмена ими. Сформулированы основные проблемы применения динамических потоков данных об угрозах в условиях изменяемых векторов атак и определены возможные направления их решения. Определены механизмы извлечения и эффективного использования контекста индикаторов компрометации для выявления инцидентов и обогащения данных при расследовании, а также возможность применения существующих методов ранжирования данных об угрозах и для обеспечения защиты киберфизических систем.

1. Современные направления и методы кибербразведки

Стремительное развитие ИТ-технологий влечет за собой и совершенствование методов кибербразведки (threat intelligence, TI) [1]. Список применяемых на практике инструментов обновляется так быстро, что публикации в литературе не успевают освещать все актуальные форматы и стандарты для работы с такими данными. Тем не менее, подобные публикации обеспечивают качественную базу для исследований, посвященных систематизации проблем и направлений развития в этой отрасли. Ниже представлен обзор публикаций, результаты которого позволили систематизировать типы источников данных кибербразведки, а также стандартов индикаторов компрометации и форматов обмена ими между различными системами.

Исследования [2, 3] посвящены обзору рынка ПО и технологий передачи индикаторов. При этом в [2] основной фокус нацелен на отношения между поставщиками TI и их влиянию на механизмы обмена информацией, а в [3] проведен подробный анализ платформ и протоколов обмена информацией об угрозах. Оба исследования свидетельствуют о том, что в отрасли кибербразведки отсутствует единое решение в части стандартизации обмена информацией между различными платформами. При этом стандарт STIX является доминирующим для этой индустрии.

В статье [4] авторы формулируют тезис о том, что для повышения эффективности противодействия злоумышленникам необходимо получать и агрегировать огромное количество информации об угрозах, что обуславливает проблемы ее обработки. Исследование описывает подход, основанный на понимании предполагаемой цели атаки, при котором данные кибербразведки фильтруются с учетом специфики работы организации, наиболее вероятных угроз внутри ее инфраструктуры и ландшафта угроз в целом. Для этого полученные данные должны обогащаться из многих источников, а процесс обмена и обогащения должен быть контролируемым и защищенным. В статье авторы рассматривают стандарты и форматы обмена индикаторами компрометации и делают вывод, что именно внедрение STIX и TAXII [2] в промышленных

масштабах стало отправной точкой развития современных TI-платформ.

В то же время в исследовании [5] предложен альтернативный подход к ранжированию и оценке релевантности источников данных киберразведки. Он основан на непрерывных наблюдениях за активностью в сети и построен на выявлении трендов появления, всплеска и исчезновения индикаторов на наблюдаемом ландшафте. Авторы позиционируют свой метод как механизм раннего обнаружения и предупреждения кибератак на защищаемый объект.

Аналогичный подход предложен в [6], однако здесь авторы предлагают расширить таксономию при обмене данными threat intelligence и выделять такие сущности, как: уязвимости, угрозы, контрмеры, атаки, риски и активы. И именно к этим объектам применяются методы анализа и контроля за активностью их упоминания в сети, в т.ч. на форумах, сайтах производителей, профильных новостных порталах и т.д. Для этого рассматриваются варианты использования как структурированных, так неструктурированных источников, ориентируясь в первую очередь на возможность нахождения актуального контекста угроз.

Статья [7] затрагивает вопросы поиска данных киберразведки в веб-среде. По результатам авторы делают вывод, что использование материала из научных публикаций малоэффективно, поскольку данная отрасль динамична и неустойчива. По их мнению, именно оперативные сводки и подборки материалов, публикуемые на динамической основе, являются одним из основных инструментов для поставщиков подобной информации.

Похожий тезис описан в [8], где авторы приводят анализ научных работ и механизмов обмена данными киберразведки и дают заключение, что наиболее актуальными являются методы, позволяющие обеспечить баланс между митигацией рисков и нарушением конфиденциальности при обмене индикаторами компрометации совместно с контекстом их применения. В отличие от вышеупомянутого подхода в данной статье основной фокус направлен на проверку и обогащение индикаторов данными из различных открытых источников.

В [9] представлено исследование, посвященное техническим аспектам анализа киберугроз. Предложена классификация типов разведданных, сформулированы преимущества обмена подобной информацией, а также факторы, которые могут обусловить отказ от тиражирования и распространения индикаторов компрометации. Авторы затрагивают вопрос соотношения объема данных киберразведки и качества содержащейся в них информации, возможных ограничений в обмене ими между платформами, а также форматов подобных данных. Это исследование дополняет упомянутые выше работы в части формулировки проблем качества данных threat intelligence и их релевантности для защищаемых объектов. В статье представлена классификация видов киберразведки на стратегический, оперативный, тактический и технический уровни, согласно которой в зависимости от уровня требуются различные механизмы не только хранения и обмена данными, но их ранжирования и анализа для предупреждения и противодействия атакам.

В работах [10, 11] представлен подробный анализ стандартов обмена индикаторами компрометации, а также вариантов таксономии для формирования отчета об инцидентах. В каждой из статей с разных сторон рассмотрены такие стандарты как MAEC [1], IODEF [5], VERIS [6], X-ARF [8], STIX и OpenIOC [2]. При этом анализ проводился с учетом различных подмножеств атрибутов и характеристик этих стандартов. Например, в работе [19] основной фокус сосредоточен на общих критериях оценки качества индикаторов, таких как: возможность автоматизированной и ручной обработки, возможность расширения, обогащения и агрегации данных, вопросов лицензирования, наличия документации и затрат на эксплуатацию. В то время как вопросам содержательности технических данных уделено меньше внимания.

В статье [11] напротив наибольшее внимание уделено вышеуказанным стандартам с точки зрения технических критериев. И именно их рассмотрение позволило авторам сформулировать такие критерии, как личность, мотивация, цель, индикатор компрометации, инструментарий, целевой объект атаки, стратегия и тактика злоумышленника, а на их основе провести сравнение стандартов на качественном уровне, абстрагируясь от технических деталей. Также в статье проведено сравнение таксономий CVE, CWE, CVSS [12] и ряда других методологий.

Исследования [13, 14] посвящены стандартам threat intelligence, но ориентированы в первую очередь на анализ онтологий, заложенных в них. Авторы дают методические указания по применению исследуемых стандартов для определения семантики угроз и формирования актуальной картины угроз для защищаемого объекта.

Несмотря на то, что в большинстве работ речь шла об универсальности применения стандарта STIX 1.x, в статьях [15, 16] отражены несколько критичных аспектов при обмене и совместном использовании данных киберразведки. К ним относятся юридиче-

ские вопросы в части нарушения конфиденциальности информации, в том числе при трансграничном обмене индикаторами между разными юрисдикциями. Общий мотив этих работ состоит в том, что зачастую несовместимые требования разных юрисдикций являются препятствием для создания единых платформ обмена индикаторами, решающими не только технические проблемы обработки информации, но и юридические противоречия.

В [17] рассмотрены практические аспекты совместного использования данных threat intelligence и в результате сформирована классификация блокирующих факторов данного процесса, включая операционные, организационные, экономические и политические. Также рассмотрены факторы, влияющие на качество релевантность индикаторов компрометации, риск нарушения конфиденциальности и затраты на создание инфраструктуры для подобного процесса.

Проблема отсутствия универсальной платформы также затронута в [18], при этом одним из вариантов решения рассматривается платформа MISP [3]. Рассмотрен веб-интерфейс платформы и особенности представления информации об угрозах. Подробно описаны технические решения, необходимые для ее использования, а также процесс синхронизации распространяемой через нее информации, используемая таксономия и возможности ее расширения.

2. Типы источников threat intelligence

Анализ литературы показал, что одним из основных терминов в отрасли кибербразведки является индикатор компрометации. Именно на обнаружении и анализе подобных индикаторов сфокусированы современные методы проактивного поиска угроз.

Индикаторы компрометации – технологические данные, которые непосредственно используются системами и компонентами киберзащиты для обнаружения вредоносных или подозрительных действий. Основным свойством любого индикатора компрометации являются конкретные технические артефакты, которые могут использоваться для выявления подозрительной активности в работе защищаемой инфраструктуры. В то же время наиболее ценные индикаторы помимо технических артефактов включают в себя информацию о контексте в дополнение к поведенческим, вычисляемым или другим атомарным характеристикам, позволяющую оценить применимость индикатора в конкретной ситуации.

В рамках настоящего исследования под контекстом понимается дополнительное описание угрозы, которую несет индикатор. Контекст может содержаться в самом отчете, репозитории, публикации в социальной сети, либо в описании на сайте источника. Контекст может включать в себя название вредоносного ПО, название группировок атакующих, пострадавших компаний или отраслей, где применяется атака.

Подобные индикаторы часто упоминаются как фиды [8]. Наиболее простой способ представления контекста – текстовое поле, содержащее описание в свободной форме любой информации, связанной с данным индикатором (время первого обнаружения, связь с определенными группировками злоумышленников и другими индикаторами). В случае подобного подхода обработка контекста значительно осложняется, так как отсутствует возможность автоматизированного анализа таких полей и определения возможности применения и ценность отдельного индикатора для конкретной инфраструктуры. Среди наиболее распространенных проблем можно выделить синтаксические ошибки в названиях, а также синонимы имен вредоносного ПО и группировок. В результате анализа вышеупомянутой литературы, а также собственных исследований авторов было выделено несколько типов источников данных для кибрерразведки: внутренние источники, внешние модерируемые источники и внешние открытые источники.

2.1. Внутренние источники

Данные кибербразведки могут быть получены из различных систем и СЗИ как результат наблюдения за происходящими внутри защищаемой инфраструктуры событиями. В первую очередь речь идет об атомарных индикаторах [19], зафиксированных СЗИ. При этом подразумеваются не только периметральные СЗИ, но и средства контроля доступа между внутренними сегментами, а также средства защиты конечных точек. При этом наблюдение таких событий во времени позволяет накапливать статистику и определять шаблоны штатной работы системы, чтобы в последствии выявлять инциденты на основе обнаруженных отклонений в поведении объектов. В таблице 1 представлены виды внутренних источников получения IoC. Детальная информация представлена ниже.

Журналы регистрации событий систем и приложений

На сегодняшний день все операционные системы и приложения имеют развитые подсистемы регистрации событий, которые позволяют контролировать происходящие на хостах события. В большинстве случаев эти данные централизуются в системах управления

Таблица 1

Виды внутренних источников получения индикаторов компрометации

Источник киберразведки	Системы	Описание
Журналы регистрации событий	Все системы	Активность пользователей и служб, ошибки в работе программного обеспечения и события аудита безопасности
Сетевые события	Межсетевые экраны, маршрутизаторы, коммутаторы	Регистрация сетевых соединений, уведомления о срабатывании правил ограничения доступа, успешные и неуспешные попытки аутентификации
Профили сетевого трафика	Коммутаторы, маршрутизаторы, активное сетевое оборудование	Уведомления о превышении показателей по нагрузке, SNMP-трапы, метаданные траффика
Уведомления от периметральных средств защиты	Системы обнаружения и предотвращения вторжений, межсетевые экраны различного уровня	Уведомления и события обнаружения аномалий
Уведомления средств антивирусной защиты и системы обнаружения вторжений уровня хоста	Средства управления антивирусной защитой и системы защиты конечных точек	Уведомления об обнаружении вредоносного ПО и аномального использования системных утилит
Сотрудники	Все системы	Сообщения от пользователей и администраторов об аномальной работе систем
Внутренние расследования	Все системы	Индикаторы и артефакты, собранные в результате внутренних расследований инцидентов

событиями безопасности (SIEM) [20], позволяющих нормализовать и фильтровать данные. Применение такого подхода обеспечивает возможность активно пополнять и обновлять данные киберразведки из источников внутри самой сети.

Сетевые средства защиты информации. Все современные сетевые устройства также позволяют отслеживать происходящие события, в т.ч. факты сетевых соединений, срабатывания правил контроля доступа, попытки неуспешного входа и т.д. Несмотря на то, что эти данные также могут быть перенаправлены в SIEM, этот вид устройств стоит отнести к отдельным источникам индикаторов компрометации, потому что они могут генерировать их и самостоятельно поставлять в TI-платформы (например, посылать SNMP-трапы или сообщения на электронную почту при определенных событиях).

Сетевой трафик

Сам трафик представляет собой отдельный источник данных для киберразведки. Во-первых, на основе статистических данных можно строить профили нормальной работы и взаимодействия внутри систем и при выявлении отклонений определять некоторые индикаторы компрометации. При этом могут быть использованы как простейшие показатели на базе протоколов SNMP [20] или RMON [9], так и метаданные самого трафика, из которого извлекаются IP-адреса, порты и технические артефакты. Во-вторых, используя технологии глубокого анализа трафика (deep packet inspection, DPI) [21], можно извлекать индикаторы из протоколов прикладного уровня и классифицировать их для дальнейшего использования в проактивном поиске угроз.

Периметральные средства защиты

Среди сетевых средств защиты отдельно можно выделить класс пограничных устройств, у которых есть собственные механизмы выявления угроз. К этому классу относятся системы обнаружения и предотвращения вторжений и межсетевые экраны уровня приложений. Зачастую они имеют собственные консоли для управления правилами детектирования, на основе которых можно отправлять уведомления в SIEM или напрямую в TI-платформу.

Антивирусы и системы защиты конечных точек

В большинстве компаний системы антивирусной защиты имеют один или несколько серверов управления, где агрегируются события об обнаружении вредоносного ПО на всех хостах. В случае использования

Рис. 1. Предлагаемая классификация внутренних источников индикаторов компрометации

модулей или систем защиты конечных точек (endpoint detection and response, EDR), помимо сигнатурных механизмов детектирования и контроля файлов, появляются данные о подозрительных процессах в оперативной памяти и аномальной работы легитимного ПО. Все эти данные могут быть использованы для извлечения индикаторов компрометации и также направлены в SIEM или TI-платформу.

Сотрудники

Если в организации выстроена работа в части профилактики киберугроз, то нередко именно пользователи и сотрудники, не имеющие напрямую отношения к информационной безопасности, могут обращать внимание и сообщать о нештатной работе систем или наличии подозрительных событий (например, странном поведении операционной системы или получении подозрительного письма на электронную почту). Отчеты, сообщения от пользователей в таком случае становятся одним из значимых источников для внутренней кибербразведки и поиска индикаторов компрометации.

Форензика по результатам расследования инцидентов

В данном случае подразумевается, что результаты расследования каждого инцидента внутри сети, должны подвергаться анализу на предмет выделения из них данных для кибербразведки. Анализ журналов событий, сетевых взаимодействий и уведомлений от других СЗИ может предоставить широкие возможности для описания тактик, техник и процедур злоумышленников, которые были использованы при этой атаке. Полученные индикаторы и понимания цепочек действий могут быть использованы для разработки новых сценариев детектирования и предотвращения похожих инцидентов в дальнейшем.

В ходе исследования различных внутренних источников IoC авторами сформирована классификация индикаторов по источникам их получения, представленная на рисунке 1. По итогам классификации были выделены хостовые, сетевые и поведенческие индикаторы.

Несмотря на то, что внутренняя инфраструктура является наиболее доступной средой получения данных кибербразведки, подобные процессы на практике применяются крайне редко. В первую очередь, это обусловлено значительными трудозатратами на извлечение и обработку данных. Для эффективного решения такой задачи помимо персонала, обслуживающего непосредственно СЗИ, необходимо нанимать в штат специалистов для анализа и практического применения подобной информации. Но даже если такой персонал есть, то в инфраструктурах с высоким уровнем защищенности инцидентов не так много и

зачастую они однотипны. Поэтому выстраивание процесса threat intelligence несомненно требует использование и других типов источников. При этом к проведению киберразведки внутри и работе с внутренними источниками приступают на достаточно высоком уровне зрелости других процессов информационной безопасности.

Далее будут рассмотрены внешние источники данных для киберразведки, которые можно разделить на два класса: модерируемые (регулярно обновляемые некоторыми поставщиками) и получаемые в состоянии «как есть» (в основном получаемые из общедоступных ресурсов).

2.2. Внешние модерируемые источники

Модерация источников IoC подразумевает их регулярное обновление и актуализацию с учетом возможного устаревания индикаторов, а также смены статуса (например, IP-адрес может перестать быть индикатором компрометации после устранения источника вредоносной активности на этом ресурсе). При этом периоды актуализации могут значительно отличаться в зависимости от источника. Здесь можно выделить два основных вида источников: коммерческие продукты (услуги поставки данных об угрозах) и бесплатные источники индикаторов компрометации.

В большинстве случаев наименьшие периоды модерации фидов характерны для коммерческих проектов, но и в случае бесплатных ресурсов встречаются часто обновляемые и актуальные данные. В связи с ограничениями подписок на платные ресурсы основное направление исследования было сосредоточено на открытых и бесплатных источниках индикаторов компрометации. Это ресурсы, поддерживаемые открытыми сообществами исследователей в области информационной безопасности, делящихся своими наработками по выявлению и изучению вредоносного ПО, а также техник и тактик злоумышленников. Такие фиды в основном содержат IP-адреса, домены, URL-адреса, имена и хеш-суммы файлов. Основным вариантом их применения является изучение использование полученных атомарных индикаторов для создания правил межсетевых экранов, сетевых и хостовых IDS [22], а также систем класса SIEM, чтобы блокировать или уведомлять о появлении индикатора в процессе работы защищаемого объекта.

В ходе исследования было в сети Интернет было обнаружено более 300 открытых источников индикаторов компрометации, из которых 130 имели период модерации не более 6 месяцев. Данные источники были отобраны для исследования как наиболее релевантные и актуальные. Также при выборе объектов исследования предпочтения отдавались источникам, поставляющим данные, придерживаясь определенного стандарта. В ряде случаев для получения данных использовались готовое клиентское ПО, в других вариантах применялись собственные скрипты для автоматизации загрузки индикаторов.

Стоит отметить, что некоторые TI-поставщики, например, abuse.ch, поставляют несколько различных потоков данных. При этом часть этих потоков дублируются и ретранслируются другими источниками (агрегаторами) индикаторов компрометации. Например, часть данных канала abuse.ch дублируется через Malware Bazaar и URLhaus. В них ретранслируются данные об образцах вредоносного ПО, URL-адресах, используемыми для его распространения вредоносных программ, черных списков SSL-сертификатов, используемых центрами управления ботнет-сетями. На рисунке 2 представлен пример данных, получаемых с

```
##################################################################
# abuse.ch SSLBL SSL Certificate Blacklist (SHA1 Fingerprints) #
# Last updated: 2022-10-10 14:21:37 UTC                        #
#                                                              #
# Terms Of Use: https://sslbl.abuse.ch/blacklist/              #
# For questions please contact sslbl [at] abuse.ch             #
##################################################################
#
# Listingdate,SHA1,Listingreason
2022-10-10 14:21:37,a56ced67e43bd667f829161a91d487016ffb9672,Vjw0rm C&C
2022-10-10 07:34:05,3a719d77508b45fbc422471d2059ef79ff558a4d,AsyncRAT C&C
2022-10-10 07:32:43,f04a75e6507173faeec2bb82c564030a5e8413ff,QuasarRAT C&C
2022-10-10 07:32:18,78436c6a8632250c2b598d0695b92669126abb74,QuasarRAT C&C
```

Рис 2. Пример фида abuse

```
; Spamhaus EDROP List 2022/10/11 - (c) 2022 The Spamhaus Project
; https://www.spamhaus.org/drop/edrop.txt
; Last-Modified: Wed, 21 Sep 2022 08:26:49 GMT
; Expires: Wed, 12 Oct 2022 04:40:18 GMT
2.56.58.0/24 ; SBL578519
5.188.11.0/24 ; SBL402809
27.112.32.0/19 ; SBL237955
31.210.20.0/24 ; SBL545365
45.91.227.0/24 ; SBL508101
45.133.200.0/24 ; SBL552797
45.143.136.0/24 ; SBL550369
```

Рис 3. Пример Spamhaus

источника abuse.ch.

Другой поставщик данных – blockikist.de – агрегирует отчеты от многочисленных серверов по всему миру, которые блокируют аномальную активность с помощью обучаемых решений. Агрегированные данные можно скачать напрямую или получить через API-запросы в виде простого списка ip-адресов. Также данная информация может быть получена через dns-запросы в виде черных списков DNS. При этом данные, поставляемые через blocklist.de, не содержат контекст и не могут быть обогащены через другие источники. То есть упоминание в базе IP-адреса не дает возможности оценить, какая именно аномальная активность с ним связана. Зачастую это могут быть только попытки подбора пароля по одному из протоколов SSH, FTP, IMAP и др., не имеющие отношения к конкретным группировкам или кампаниям.

Аналогичные данные также предоставляет ресурс Spamhaus: агрегирует и распространяет списки IP-адресов, с которых была зафиксирована рассылка спам-писем или на них обнаружено использование эксплойтов. Кроме того, у данного поставщика имеются обновляемые списки IP-адресов, которые можно использовать на пограничных маршрутизаторах для блокировки нелегитимного трафика. Пример фидов Spamhaus представлен на рис. 3.

2.3. Внешние открытые источники

К этому типу источников данных киберразведки чаще всего относят открытые источники (Open source intelligence, OSINT) [23], которые позволяют понять ландшафт угрозы, связанной с определенными индикаторами компрометации. В большинстве случаев такие источники ориентированы на восприятие человеком, нежели машиной и часто представлены в неструктурированном виде. Примером могут быть отчеты компаний об утечках данных или обнаруженных уязвимостях, доклады на профильных конференциях, обнародовавшие новые техники и механизмы атак. Информация, получаемая из такого типа источников, в большей степени относится к стратегическому уровню киберразведки.

Сюда же можно отнести средства массовой информации (СМИ), социальные сети и мессенджеры, в которых максимально оперативно распространяются новости. Набор свободно распространяемого инструментария для автоматизированного поиска IoC в таких источниках весьма широк. Помимо специализированных утилит на сегодняшний день высоко развиты технологии автоматизированного парсинга сообщений в мессенджерах и исследования вебстраниц с помощью краулеров. Но в большинстве случае извлечение индикаторов из них значительно затруднено по причине отсутствия структурированной формы данных. В таблице 2 приведены примеры подобных источников.

Также существует ряд источников, которые выпускают регулярные отчеты и уведомления об уязвимостях в стандартизированном виде. Такие отчеты обычно содержат данные об актуальных уязвимостях и оформляются в соответствии с CVRF (Common vulnerability reporting framework). При этом используются шкалы оценки, например, CVSS [9], исходя из значений, которых можно формировать планы по устранению уязвимостей и организации проактивного поиска угроз. Примерами подобных источников являются официальные порталы с рекомендациями по безопасности таких вендоров как: Cisco, Microsoft, Oracle, Red Hat и др. Принципиальное отличие подобных открытых источников состоит в наличии не только контекста и описания

Таблица 2

Примеры внешних открытых источников

Источник	Описание
Новостные каналы	Статьи с описанием новых угроз
Уязвимости	Уведомления и бюллетени
Специализированные поисковые системы	Поиск уязвимых систем (Shodan, Censys)
Вендоры АВЗ и EDR	Отчеты, уведомления, рассылки
Мессенджеры	Обмен информацией в чатах и каналах
Даркнет	Поиск информации в закрытых сообществах

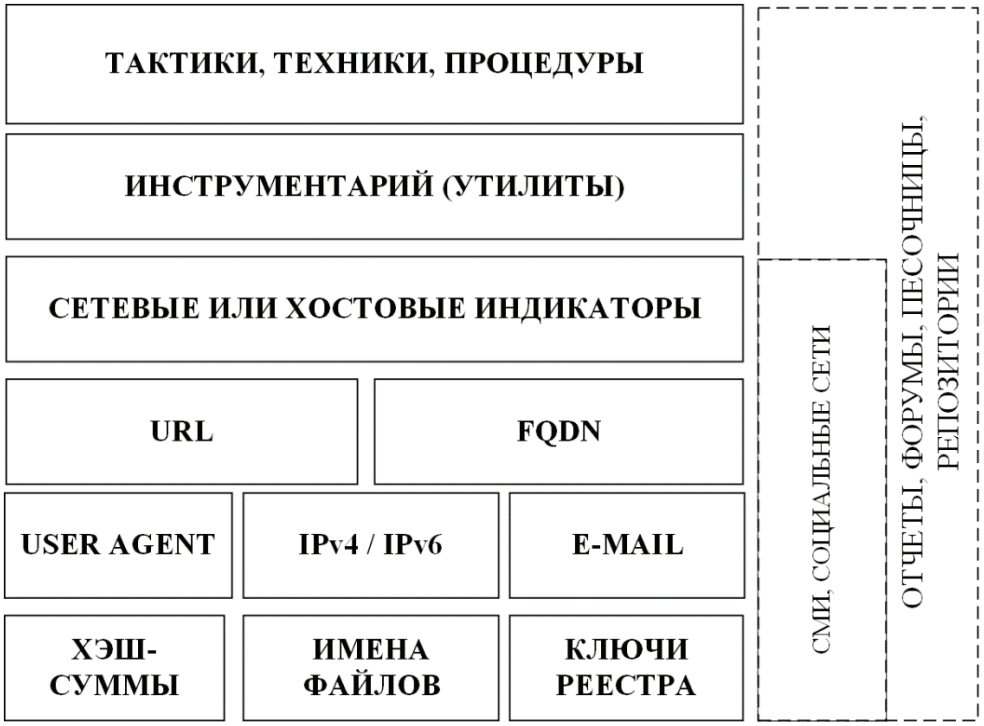


Рис. 4. Распределение источников по типам индикаторов

ландшафта угрозы, но и зачастую описания мер по их митигации, сведений об исправлениях и ссылок на загрузку необходимых патчей.

Стоит отметить, что одним из наиболее актуальных подходов к поиску индикаторов компрометации также является исследование «теневого интернета» (darknet) [7, 19]. Здесь есть ряд сложностей, связанных с нестабильностью подключений к TOR-нодам, и закрытостью сообществ и форумов в данном сегменте. В большинстве случаев для получения информации на таких площадках необходимо проходить процедуру проверки и подтверждения от других пользователей. Именно поэтому изучение подобных источников обычно реализуется либо в крупных компаниях, способных позволить содержание выделенного квалифицированного специалиста на эту задачу, либо поставщиками данных кибербразведки, для которых данный вид деятельности является основным.

В ходе исследования различных OSINT платформ по обмену индикаторами компрометации авторами была описана структура распределения индикаторов, не только отражающая источники их получения, но и позволяющая определить ценность IoC согласно модели The Pyramid of Pain, предложенной в [24]. На рис. 4 представлено распределение источников индикаторов компрометации в соответствии с уровнями данной модели.

3. Стандарты обмена индикаторами компрометации

Большинство форматов для обмена индикаторами компрометации были определены в ходе научного обзора и практических изысканий в описанных выше источниках. В некоторых случаях были изучены и рассмотрены готовые инструменты для работы с данными, предоставляемыми самими поставщиками данных кибербразведки. В случае с открытыми источниками применялись сторонние утилиты или собственные скрипты. По итогам исследования выделены следующие категории:

- специализированные стандарты, ориентированные на threat intelligence, принятые некоторыми сообществами и обсуждаемые в сети;
- частные форматы, предлагаемые отдельными поставщиками индикаторов компрометации;
- общие форматы, часто используемые для распространения другой информации, в т.ч. не относящейся к кибербразведке;
- исторически сохранившиеся форматы, изредка упоминаемые в литературе, но редко используемые на практике при обмене индикаторами компрометации.

3.1. Специализированные стандарты threat intelligence

Наиболее известным специализированным форматом для обмена данными кибербразведки является STIX, первая версия которого была принята в 2012г. Основной целью при разработке данного формата стала возможность гибкого представления данных, чтобы агрегировать их вместо дублирования. Применение для этого XML позволило решить задачу, но привело к большому уровню вложенности. В результате была разработана новая версия стандарта STIX2.1. Помимо самого стандарта для описания данных разработан также транспортный механизм TAXII, который является предпочтительным, но не обязательным транспортным механизмом для STIX. При этом для каждой версии STIX существуют разные версии TAXII, несовместимые друг с другом. Принципиальные различия между STIX 2.x и STIX 1.x заключаются в сериализации и переходе от формата XML к JSON [25], что позволило и оптимизировать поиск по массивам данных. Оптимизация достигается за счет плоской структуры данных. Дополнительно стандарт предусматривает описание объектов домена, определенными на верхнем уровне документа для упрощения синтаксического анализа и хранения. При этом взаимосвязь между SDO обеспечивается введением объекта отношений STIX.

Известен также стандарт CybOX [2], который изначально был разработан для описания событий, зафиксированных в результате наблюдений за инцидентами, но с появлением STIX 2.1 был интегрирован в него и стал частью стандарта STIX вместе со стандартом MAEC [2]. Последняя версия MAEC 5.0, модифицированная для описания вредоносного ПО с использованием таких атрибутов, как поведение, артефакты и взаимосвязи между образцами ПО, также была включена в STIX 2.1 и применяется для наблюдаемых объектов. MAEC имеет хорошую поддержку и часто применяется вендорами потоковых песочниц. В то же время и нередко наблюдаются проблемы при использовании разных версий стандарта и API-интерфейсов [1], специфичных для конкретной платформы. Вышеупомянутая версия MAEC 5.0 использует для описания данных такие же механизмы, как и STIX 2.1, однако в ходе исследования случаев взаимной поддержки между стандартами обнаружено не было.

CVRF [8] – это еще один стандарт IoC, представленный в машиночитаемом формате и ориентированный автоматизацию распространения рекомендаций и отчетов об уязвимостях. Указанный стандарт позволяет удовлетворить реализовать обмен информацией об уязвимостях с возможностью версионирования, что обеспечит высокую эффективность при анализе отдельных уязвимостей. Среди недостатков стандарта можно отметить ограниченное соответствие требованиям со стороны многих поставщиков threat intelligence основных влиятельных лиц и наличие в формате многочисленными схожих по смыслу таксономических полей. В настоящее время стандарт CVRF используется репозиторием уязвимостей CVE MITRE [14], а также активно поддерживается такими вендорами как: Cisco, Oracle и Red Hat. В связи с этим CVRF может стать одним из лидирующих стандартов для распространения уязвимостей и рекомендаций по безопасности.

3.2. Стандарты, разработанные поставщиками данных кибербразведки

Среди применяемых на практике стандартов описания индикаторов, созданными непосредственно поставщиками фидов можно выделить как вендорозависимые, например, IDEA [23], MISP [25] и CIF [5], так и универсальные, применяемые несколькими вендорами в схожих по функционалу продуктах.

IDEA был разработан компанией CESNET, управляющей крупной сетевой инфраструктурой и предостав-

ляющей услуги высшим учебным заведениям и исследовательским учреждениям в Чешской Республике. Стандарт ориентирован на обмен данными киберразведки, которые различаются по своей природе, поэтому структура данных должна быть гибкой, расширяемой и при этом оставаться простой. Основной целью было снижение сложности применения стандарта и повышение гибкости представления данных по сравнению с другими форматами.

Формат MISP – это собственный протокол для связи между экземплярами платформы MISP. Представляет собой JSON обладает гибкими возможностями расширения и широко используется на практике. Характеризуется широкой распространенностью (в рамках проекта MISP известно более 6000 платформ, что свидетельствует о широкой поддержке как в общественных, так и в государственных организациях).

Формат CIF [5] – еще одна широко используемая платформа для агрегирования и совместного использования данных киберразведки, которая предоставляет свою разновидность представления IoC в формате JSON.

Помимо вендорозависимых стандартов стоит отметить класс решений по обнаружению и предотвращению вторжений, в котором многие производители не стремятся создавать свои языки формализованного описания, чтобы обеспечить взаимозаменяемость продуктов. В том числе, сюда относятся правила IDS/IPS в форматах Snort [14] и Suricata [14]. Формат их написания характеризуется тем, может напрямую использоваться большим количество программных и аппаратных решений.

3.3. Общие форматы

Стоит отметить, что зачастую для передачи данных threat intelligence используются широко распространенные форматы данных общего назначения. Эти форматы никогда не разрабатывались и не предназначались для использования в качестве средства обмена индикаторами компрометации, но подходят для передачи подобной информации и широко используются для обмена IoC. К подобным форматам можно отнести список блокировок DNS (DNSBL) [6], RSS [26] и обычный текст.

В отличие от привычного текста, передача списков DNSBL организована в виде «запрос – ответ» на основе протокола DNS. Запросы позволяют определить наличие IP-адреса или домена в одном из черных списков. Технология DNSBL, возможно, является одним из старейших механизмов обмена индикаторами компрометации и чаще всего используется для защиты электронной почты в составе антиспам-фильтров и потоковых антивирусов. Также одним из распространенных форматов подобного класса является Really simple syndication (RSS) [26]. Это облегченный XML-формат, предназначенный для распространения новостей. Благодаря широкому распространению данная технология нашла применение в несколькими крупных источниках для распространения данных TI.

Тем не менее, самым распространенным форматом для обмена IoC остается текст. Данные могут поставляться в неструктурированном формате (заметки, цитаты из постов в социальных сетях и т.д.), в виде структурированного текста (например, в формате CSV [26]; списка IP или URL-адресов в один столбец), а также слабоструктурированном виде (в этом случае информация разбивается систематизируется в нескольких строках, но при этом отсутствует четко определенная схема данных). Применение текстового формата отличается высокой эффективностью и компактностью. При этом большое количество СЗИ формируют результаты своей работы именно в виде текстовых данных и процесс извлечения индикаторов компрометации из них часто сводится к использованию несложных регулярных выражений, что не требует больших вычислительных ресурсов.

3.4. Исторически сохранившиеся форматы

В ходе исследования был обнаружен ряд форматов, отраженных в литературе или заявленных в документации некоторых поставщиков IoC, но не применяемых на практике.

Например, стандарт OpenIOC [27] был разработан компанией Mandiant Inc. для проекта openioc.org с целью обеспечить общую методологию и формат для описания индикаторов компрометации на основе хоста или сети. В репозитории GitHub доступны разработанные вендором утилиты для применения данного формата, но за несколько лет в ветке не зафиксировано существенной активности [49].

Основанный на XML формат IODEF был разработан IETF для обмена данными между группами реагирования на инциденты и закреплен в RFC 5070. Несмотря на обновление версии стандарта в 2016 году и определения для него нового RFC 7970, за последние 5 лет отсутствует информация о какой-либо поддержке стандарта и не зафиксированы источники, применяющие его для распространения IoC.

Известен также формат Open threat partner exchange (OpenTPX) [28, 29], в основе которого лежит схема JSON. Характерной особенностью является

высокий уровень документированности всех параметров и открытый исходный код инструментария, предназначенный для совместного использования индикаторов. Несмотря на все достоинства среди анализируемых источников, имеющих актуальные обновления контента, не удалось обнаружить каналы, поставляющие индикаторы в данном формате.

4. Анализ источников данных киберразведки

Поскольку получение индикаторов компрометации из внутренних источников в большинстве случаев относится к проприеритарным технологиями и зачастую поставляется на рынок уже как результат в виде платных услуг, то основной фокус исследования был сосредоточен на анализе внешних открытых источников данных.

Как упоминалось ранее, характерной особенностью такого вида источников является отсутствие какой-либо типизации при определении контекста. Например, описание уязвимостей в формате CVE широко распространенный подход. В сети известно много порталов, распространяющих информацию об обнаруженных уязвимостях в этом формате. Однако существенным недостатком является ограниченная применимость таких данных для автоматизированной обработки и практическом использовании ее при разработке контента СЗИ, так как детальное описание уязвимости и подверженность ей определенных версий сильно разнятся в зависимости от источника. В то же время некоторые поставщики IoC предоставляют достаточно полное описание уязвимости в отношении применимых версий ПО. Таким образом, в большинстве случаев обработка индикаторов компрометации из подобных источников требует ручного процесса для преобразования данных в машиночитаемый формат и накладывает некоторые ограничения. Также стоит отметить, что данные, полученные из darknet сопровождались контекстом сомнительного качества, требующего тщательной проверки. В первую очередь это обусловлено ограниченным доступом к площадкам на подобных ресурсах. Тем не менее, индикаторы, полученные таким путем, не могут быть игнорированы как источник информации о киберразведке, поскольку именно в этом сегменте сосредоточена значительная часть вредоносной активности.

Анализ исследуемых TI-источников выявил несколько различных типов форматов, в т.ч. одноколоночных и многоколоночных списков, структурированных файлов CSV и более сложные форматы, такие как STIX и RSS. Было обнаружено, что многие из источников IoC, являются результатом ретрансляции более простых текстовых каналов. В большей степени это относится к источникам, поставляющим IoC в более сложных форматах. На рисунке 5 представлены результаты анализа исследуемых источников на предмет оригинальности. Следует отметить, что в некоторых случаях реализовать достоверную проверку на предмет оригинальности было невозможно из-за многократного преобразования информации при ее ретрансляции и смене форматов.

Было обнаружено, что при агрегации и ретрансляции индикаторов некоторые данные могут быть потеряны или изменены. В основном это связано с ошибками форматирования данных, искажением дат обнаружения, дублированием или агрегацией нескольких индикаторов. Подобные трансформации существенно снижают качество данных киберразведки и повышают вероятность ошибок первого рода при работе с ними. Кроме того, зафиксированы случаи, когда источник фидов, содержащий большой массив связанных данных, разделяется и поставляется в виде отдельных не связанных между собой каналов, например списков IP-адресов, URI и т.д. На рисунке 6 представлено распределение типов индикаторов в исследуемых источниках. Наиболее распространены IP-адреса, URL-адреса, хеш-суммы файлов и описание угрозы или типа вредоносного ПО.

Поставка фидов в более сложных форматах, например, STIX, позволяет предоставить более полный набор данных по сравнению с простыми текстовыми форматами, но применение таких стандартов не всегда оправдано. Например, одна запись в RSS-канале содержит в среднем 400 Байт данных. При этом эта же запись после преобразования в формат STIX 1.1. занимает от 15 до 20 КБайт. Таким образом, очевидно, что применение XML-форматов зачастую нерационально с точки зрения объема данных.

Было проведено сравнение источников, использующих сложные форматы данных для предоставления индикаторов. Результаты показывают, что возможности форматов STIX, JSON и XML зачастую используются не в полной мере. Основная причина в том, что многие из источников агрегируют данные из других каналов и преобразуют атомарные индикаторы без указания контекста. Например, формат STIX2.x позволяет обеспечить более сжатое представление информации об индикаторе, чем предыдущие версии. Однако, среди проанализированных источников только в половине случаев все поля формата были заполнены. Чаще всего данные помещаются в атрибуты описания или заголовки вместо агрегации данных и помещения в поля дополнительных индикаторов. В случаях, когда

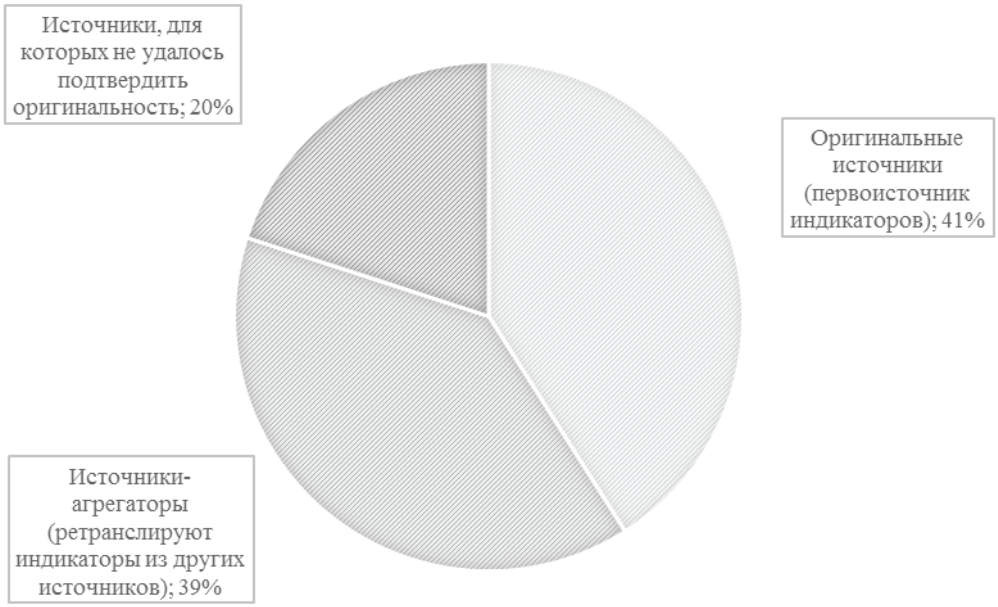


Рис. 5. Анализ повторяемости индикаторов в источниках threat intelligence

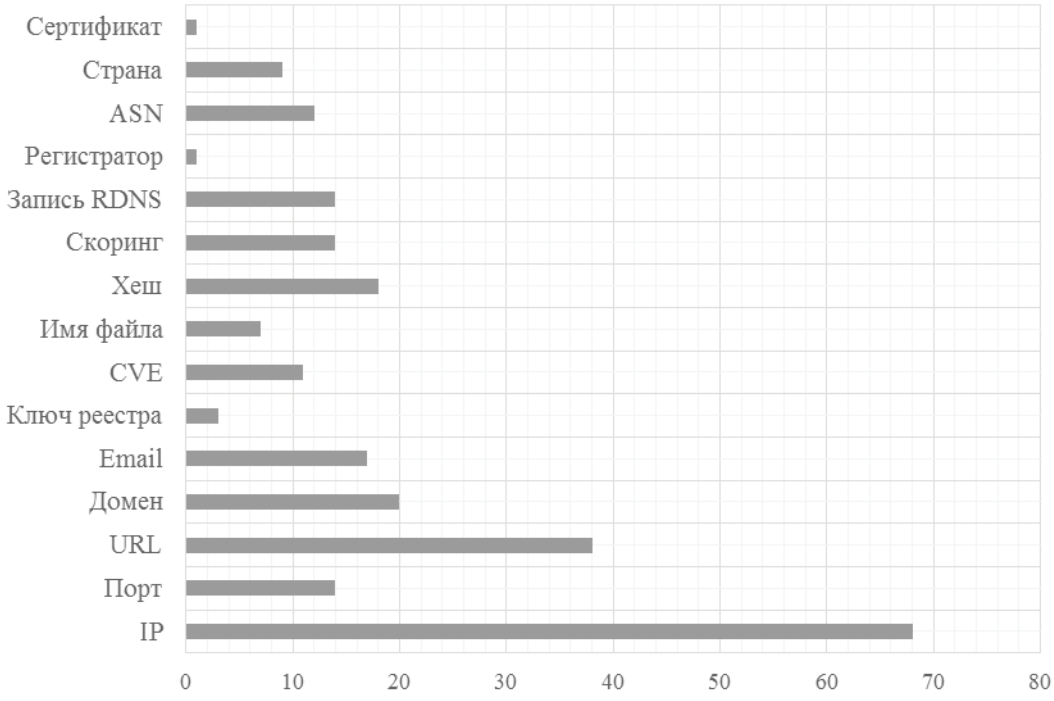
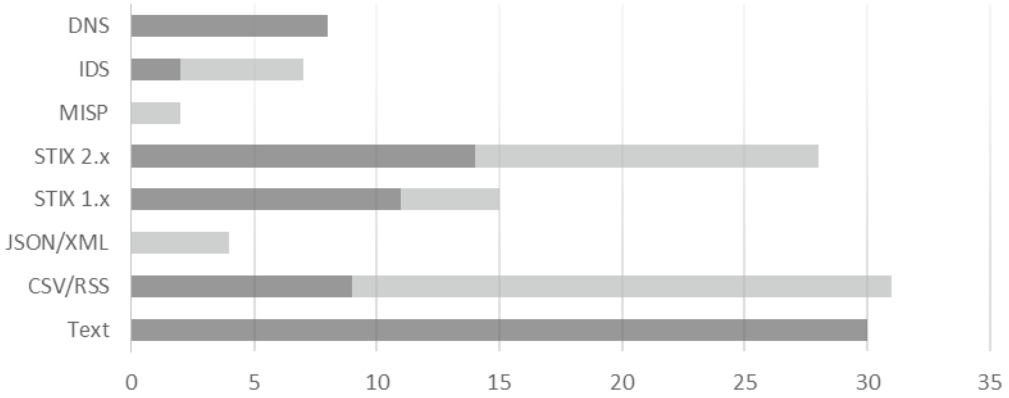


Рис. 6. Анализ повторяемости индикаторов в источниках threat intelligence

источник формирует собственные индикаторы в формате STIX, данные заполняются намного тщательнее и соответствуют идеологии стандарта.

На рис. 7 представлено соотношение случаев использования обогащенных данных и простых атомарных индикаторов в зависимости от формата как отражение эффективности его применения на практике.

Анализ источников данных киберразведки, выявленных в ходе исследования, показал, что при использовании простых форматов, таких как CSV и RSS,



	Text	CSV/RSS	JSON/XML	STIX 1.x	STIX 2.x	MISP	IDS	DNS
Соответствует стандарту	30	9	0	11	14	0	2	8
Не соответствует стандарту	0	22	4	4	14	2	5	0

Рис. 7. Анализ эффективности применения стандартов в источниках threat intelligence

индикаторы, относящиеся к одной угрозе, часто группируются на основе общей метки или тэга. В случае применения более сложных форматов, таких как STIX, используется комбинация наблюдаемых данных, шаблонов индикаторов и взаимосвязей. Объект STIX является лишь контейнером и не включает в себя отношений с другими сущностями. Для отражения взаимосвязей необходимо вводить уникальные идентификаторы и метки, что неизбежно приводит к усложнению документа и всего фида в целом.

Именно в этой области существенные преимущества дает формат MISP. Обмен данными с использованием MISP ориентирован на угрозы – файл событий содержит все индикаторы для конкретной угрозы. Идентификаторы используются для перекрестных ссылок и формирования отношений аналогично STIX. При этом структуры массивов таких атрибутов похожи на структуры массивов наблюдений STIX, однако описание взаимосвязей реализовано без дополнительных объектов, что значительно снижает сложность документа. При анализе платформ, использующих MISP, IDEA, CIF и другие аналогичные форматы было установлено, что они лучше подходят для конкретных случаев, когда необходимо описать наблюдаемые индикаторы компрометации в краткой, но исчерпывающей форме. И зачастую конечным потребителям фидов необходим именно такой подход.

При работе с открытыми платформами обмена индикаторами компрометации в рамках данного исследования был выявлен ряд проблем эффективной обработки таких данных. Поскольку решение каждой из них обуславливает несколько отдельных задач, их рассмотрение будет проведено и представлено на дальнейших этапах исследования.

К таким проблемам можно отнести трудности при подборе источников и очистке данных, нормализацию индикаторов и подбор методов извлечения контекста, вопросы обогащения данных и ранжирования при использовании нескольких каналов threat intelligence. Ниже представлены варианты решения этих проблем, примененные во время исследования, а также наиболее часто используемые на практике.

Так, при подборе источников необходимо, во-первых, минимизировать применение индикаторов от платформ-агрегаторов, поскольку они предоставляют большое количество дублируемых данных, что приводит к множеству ошибок первого рода. Во-вторых, необходимо выбирать источники с наиболее подробно заполненным контекстом. В-третьих, стоит определить частоту и время появления обновлений. Также должны быть четко сформулированы следующие операции:

— добавление индикатора;
— обновление индикатора;
— удаление индикатора.

При нормализации отчетов могут применяться как ручной анализ с извлечением значимых индикаторов и переводом их в формат, используемый в защищаемой системе, так и варианты автоматизированной обработки данных. Однако на практике даже в последнем случае необходима проверка из-за низкого качества входных данных. Среди проблем здесь можно

выделить необходимость ручной валидации результатов, частое применение скриншотов для публикации индикаторов и сложность извлечения информации о связях между индикаторами. В случаях использования из социальных сетей наиболее работоспособным механизмом нормализации можно определить применение специализированных парсеров под каждый источник. Среди проблем на этом этапе часто встречаются множественные экранирования и методы автозамены символов при публикации индикаторов в открытых источниках с целью минимизации случаев резонансного усиления их использования. Нередко имеются встречаются синтаксические и орфографические ошибки при в индикаторах.

Эффективность применения данных киберразведки можно повысить путем обогащения атомарных индикаторов путем добавления информации, которая потребуется в расследовании инцидента. Например, данные об автономной системе ASN [30, 31], геолокации IP, портах и сервисах, принадлежности сети провайдерам и т.д. Для доменных имен можно добавить данные из сервисов whois, dns lookup, а в случае URL анализировать принадлежность HTTPS-сертификата. При решении задачи обогащения зачастую невозможно осуществлять этот процесс в режиме реального времени. Необходимо некоторое время для выявления связей даже в случаях автоматизации. Часть информации, запрашиваемой из открытых источников, может быть неточной или закрытой, или же доступна только на платной основе. Кроме того, целью обогащения является получение информации, актуальной на момент обнаружения индикатора.

Немаловажной задачей является определение значимости индикаторов и оценки их отношения к угрозе. Здесь необходимы метрики, позволяющие оценить степень опасности индикатора. Среди известных методов ранжирования индикаторов можно выделить:

- оценка доверия к источникам;
- кросс-валидация индикаторов;
- категоризация угроз и назначение категориям весов;
- оценка частоты появления индикаторов в источниках.

Кроме того, все рассмотренные выше процессы характеризуются высоким уровнем ручных операций при подготовительной работе, что требует привлечения большого штата специалистов, в противном случае возникает высокая вероятность ошибок первого рода. При этом большинство рассмотренных выше исследований показывают, что не существует единого правильного подхода, и нередко для конкретных случаев применения данных киберразведки необходимо применять несколько методов или их комбинаций.

Таким образом, при организации практического использования данных киберразведки необходимо в первую очередь определить минимальный набор из доступных наборов индикаторов и производить по ним проверку на общем потоке событий. Остальные имеющиеся в распоряжении индикаторы могут быть использованы для ретроспективного поиска, а в случае их обнаружения и успешного расследования инцидента возможно расширить набор индикаторов для анализа в потоковом режиме.

Заключение

Одной из важнейших задач, закрепленных на законодательном уровне, при обеспечении надлежащей защищенности киберфизических систем является недопущение вторжения в производственные процессы, особенно запущенные в критической инфраструктуре. Эффективность обнаружения и предотвращения атак на подобные инфраструктуры требует применения механизмов, позволяющих выявлять ранее неизвестные методы и тактики действия злоумышленников.

Для решения данной задачи в сфере информационной безопасности сегодня активно формируется тренд проактивного подхода опережения действий злоумышленников с использованием методов киберразведки, среди которых наиболее распространено применение индикаторов компрометации для обогащения средств защиты киберфизических систем. Их использование также позволяет проводить действия, направленные на выявление новых, ранее неизвестных угроз и обеспечивать защиту подобных объектов на качественно новом уровне, оперируя тактиками и процедурами и предугадывая действия злоумышленников. Целью данного подхода является своевременное оповещение и предупреждение об обнаруженных аномалиях в работе системы, прямо или косвенно являющихся свидетельством инцидента безопасности.

В данной статье проведен анализ исследований за последние годы в области организации работы с источниками данных киберразведки. Рассмотрены и систематизированы источники индикаторов компрометации и предложена их классификация. Сформулированы основные проблемы обработки динамических потоков данных об угрозах в условиях изменяемых векторов атак. Определены механизмы извлечения и эффективного использования контекста индикаторов компрометации для выявления инцидентов и обога-

щения данных при расследовании, а также возможность применения существующих методов ранжирования данных об угрозах и для обеспечения защиты киберфизических систем.

Установлено, что в отрасли киберразведки на сегодняшний день отсутствует единое решение в части стандартизации обмена информацией между различными платформами, но при этом имеют место ряд доминирующих стандартов и форматов обмена подобными данными. В ходе подготовки обзора существующих стандартов рассмотрены и структурированы актуальные проблемы проактивного поиска угроз на примере открытых источников индикаторов компрометации при обработке потоков событий в системах управления событиями безопасности и предложены методы их решения. Кроме того, при работе с открытыми платформами обмена индикаторами компрометации в рамках данного исследования был выявлен ряд проблем эффективной обработки таких данных. Поскольку решение каждой из них обуславливает несколько отдельных задач, их рассмотрение будет проведено и представлено на дальнейших этапах исследования.

Работа выполнена при финансовой поддержке гранта РНФ № 22-21-00846.

Литература

1. Liao X., Yuan K., Wang Z., Li Z., Xing L., Beyah R. Acing the IOC Game: Toward Automatic Discovery and Analysis of Open-Source Cyber Threat Intelligence // Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. – 2016. – P. 755-766.
2. Sauerwein C., Sillaber C., Mussmann A., Breu R. Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives // Wirtschaftsinformatik und Angewandte Informatik. – 2017. – P. 837-851.
3. Zrahia A. Threat intelligence sharing between cybersecurity vendors: Network, dyadic, and agent views // Journal of Cybersecurity. – 2018. – Vol. 4, issue 1. – P. 1–16.
4. Brown S., Gommers J., Serrano O. From Cyber Security Information Sharing to Threat Management // Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security. – Denver, CO, USA, 12–16 October 2015. – P. 43–49.
5. Liu R., Zhao Z., Sun C., Yang X., Gong X., Zhang J. A Research and Analysis Method of Open Source Threat Intelligence Data // Communications in Computer and Information Science (CCIS). – 2017. – Vol. 727. – P. 352–363.
6. Sauerwein C., Pekaric I., Felderer M., Breu R. An analysis and classification of public information security data sources used in research and practice // Computers & Security. – 2019. – Vol. 82. – P. 140-155.
7. Abu M.S.; Selamat S.R., Ariffin A., Yusof R. Cyber Threat Intelligence – Issue and Challenges. Indones // Indonesian Journal of Electrical Engineering and Computer Science. – 2018. Vol. 10, no. 1. – P. 371–379.
8. Pala A., Zhuang J. Information sharing in cybersecurity: A review // Decision Analysis. – 2019. – Vol. 16, no. 3. – P. 172-196.
9. Tounsi W., Rais H. A survey on technical threat intelligence in the age of sophisticated cyber-attacks // Computer Security. – 2018. – Vol. 72. – P. 212–233.
10. Menges F., Pernul G. A comparative analysis of incident reporting formats // Computer Security. –2018. – Vol. 73. – P. 87-101.
11. Mavroeidis V., Bromander S. Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence // Proceedings of the 2017 European Intelligence and Security Informatics Conference (EISIC). – Athens, Greece: IEEE, 2017. – P. 91–98.
12. Skopik F. Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks at National Level. – CRC Press: Boca Raton, FL, USA, 2018. – 446 p.
13. Burger E.W., Goodman M.D., Kampanakis P., Zhu K.A. Taxonomy model for cyber threat intelligence information exchange technologies // Proceedings of the ACM Workshop on Information Sharing & Collaborative Security (WISCS). – Scottsdale, AZ, USA, 3 November 2014. – P. 51–60.
14. Asgarli E., Burger E. Semantic ontologies for cyber threat sharing standards // Proceedings of the 2016 IEEE Symposium on Technologies for Homeland Security (HST). – Waltham, MA, USA: IEEE, 2016. – P. 1-6.
15. Serrano O., Dandurand L., Brown S. On the Design of a Cyber Security Data Sharing System // Proceedings of the ACM Workshop on Information Sharing & Collaborative Security (WISCS). – Scottsdale, AZ, USA, 3 November 2014. – P. 61–69.
16. Sullivan C., Burger E. “In the public interest”: The privacy implications of international business-to-business sharing of cyber-threat intelligence // Computer Law & Security Review. – 2017. – Vol. 33, issue 1. – P. 14–29.
17. Zibak A., Simpson A. Cyber threat information sharing: Perceived benefits and barriers // Proceedings of the 14th International Conference on Availability, Reliability and Security. – Canterbury, UK, 26–29 August 2019. – P. 1–9.
18. Wagner C., Dulaunoy A., Wagener G., Iklody A. MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform // Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security. – Vienna, Austria, 24 October 2016. – P. 49-56.
19. Friedman J., Bouchard M. Definitive Guide to Cyber Threat Intelligence. – CyberEdge: Annapolis, MD, USA, 2015. – 72 p.
20. Bryant B., Saiedian H. Improving SIEM Alert Metadata Aggregation with a Novel Kill-Chain Based Classification Model // Computers & Security. – 2020. – Vol. 94. – P. 101817.
21. Shameli-Sendi A., Louafi H., He W., Cheriet M. Dynamic Optimal Countermeasure Selection for Intrusion Response System // IEEE Transactions on Dependable and Secure Computing. – 2018. – Vol. 15, no. 5. – P. 755-770.
22. Farnham G., Leune K. Tools and standards for cyber threat intelligence projects // SANS Institute. – 2013. – Vol. 3., no. 2. – P. 25-31.

23. Schaberreiter T., Kupfersberger V., Rantos K., Spyros A., Papanikolaou A., Ilioudis C., Quirchmayr G. A quantitative evaluation of trust in the quality of cyber threat intelligence sources // Proceedings of the 14th International Conference on Availability, Reliability and Security. – 2019. – P. 1-10.
24. Bianco D.J. The Pyramid of Pain [Электронный ресурс]. – 2013. – URL: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html (дата обращения: 05.08.2022).
25. Mokaddem S., Wagener G., Dulaunoy A., Iklody A. Taxonomy driven indicator scoring in MISP threat intelligence platforms [Электронный ресурс]. – 2019. – URL: https://arxiv.org/abs/1902.03914 (дата обращения: 05.08.2022).
26. Appala, S.; Cam-Winget, N.; McGrew, D.A.; Verma, J. An actionable threat intelligence system using a publish–subscribe communications model. In Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security, Denver, CO, USA, 12–16 October 2015; pp. 61–70.
27. Wagner, T.D. Cyber Threat Intelligence for "Things". In Proceedings of the 2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA), Oxford, UK, 3-4 June 2019; pp. 1–2.
28. Menges, F.; Sperl, C.; Pernul, G. Unifying cyber threat intelligence. In Trust, Privacy and Security in Digital Business (TrustBus), Lecture Notes in Computer Science; Springer: Berlin, Germany, 2019; Volume 11711, pp. 161–175.
29. Wagner T.D., Mahbub K., Palomar E., Abdallah A.E. Cyber threat intelligence sharing: Survey and research directions // Computer Security. – 2019. – Vol. 87. – P. 101589
30. Lavrova D.S. An approach to developing the SIEM system for the Internet of Things // Automatic Control and Computer Sciences. – 2016. – Vol. 50. – P. 673-681.
31. Raju B.K., Geethakumari G. Event correlation in cloud: a forensic perspective // Computing. – 2016. – Vol. 98, no. 11. – P. 1203–1224.

STUDY OF COMPROMETATION INDICATORS FOR IMPROVEMENT OF INFORMATION AND CYBERPHYSICAL SYSTEMS PROTECTION FACILITIES

Meshcheryakov Roman[3], Iskhakov Sergey[4]

Purpose of work: *study of existing standards of compromise indicators and methods of their exchange for enrichment of protection systems of information and cyber-physical systems.*

Research method: *systematic analysis of open sources of data on indicators of compromise, standards of their description and methods of exchange in the organization of cyberintelligence.*

The result obtained: *the actual problems of proactive search of threats are formulated on the example of the application of open sources of indicators of compromise in the processing of event flows in security event management systems. The classification of indicators derived from internal sources is proposed. The main problems of processing dynamic threat data streams under changing attack vectors are formulated.*

It was found that the threat intelligence industry currently lacks a unified solution in terms of standardization of information exchange between different platforms, but there are a number of dominant standards and formats of such data exchange. In the course of preparing the review of existing, the tasks of identifying previously unknown attack methods based on the use of open sources of indicators of compromise in data processing in security incident management systems were considered and structured, and methods for their solution were proposed.

Scientific novelty: *the presented article is one of the first domestic works, devoted to the analysis of research in recent years in the field of organization of work with threat intelligence data sources. Reviewed and systematized the sources of indicators of compromise and proposed their classification. Formulated the main problems of processing dynamic threat data streams under conditions of variable attack vectors.*

Keywords: *compromise indicator, cyber-intelligence, context, cyber-physical system, security event management system, enrichment, ranking.*

3 Roman V. Meshcheryakov, Dr. Sc. (in Eng.), Professor, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. E-mail: mrv@ieee.org, ORCID: 0000-0002-1129-8434

4 Sergey Yu. Iskhakov, Ph.D. (in Eng.), Promsvyazbank, Moscow, Russia. E-mail: sergey@iskhakov.ru, ORCID: 0000-0003-3346-9262

References

1. Liao X., Yuan K., Wang Z., Li Z., Xing L., Beyah R. Acing the IOC Game: Toward Automatic Discovery and Analysis of Open-Source Cyber Threat Intelligence // Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. – 2016. – P. 755-766.
2. Sauerwein C., Sillaber C., Mussmann A., Breu R. Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives // Wirtschaftsinformatik und Angewandte Informatik. – 2017. – P. 837-851.
3. Zrahia A. Threat intelligence sharing between cybersecurity vendors: Network, dyadic, and agent views // Journal of Cybersecurity. – 2018. – Vol. 4, issue 1. – P. 1–16.
4. Brown S., Gommers J., Serrano O. From Cyber Security Information Sharing to Threat Management // Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security. – Denver, CO, USA, 12–16 October 2015. – P. 43–49.
5. Liu R., Zhao Z., Sun C., Yang X., Gong X., Zhang J. A Research and Analysis Method of Open-Source Threat Intelligence Data // Communications in Computer and Information Science (CCIS). – 2017. – Vol. 727. – P. 352–363.
6. Sauerwein C., Pekaric I., Felderer M., Breu R. An analysis and classification of public information security data sources used in research and practice // Computers & Security. – 2019. – Vol. 82. – P. 140-155.
7. Abu M.S.; Selamat S.R., Ariffin A., Yusof R. Cyber Threat Intelligence – Issue and Challenges. Indones // Indonesian Journal of Electrical Engineering and Computer Science. – 2018. Vol. 10, no. 1. – P. 371–379.
8. Pala A., Zhuang J. Information sharing in cybersecurity: A review // Decision Analysis. – 2019. – Vol. 16, no. 3. – P. 172-196.
9. Tounsi W., Rais H. A survey on technical threat intelligence in the age of sophisticated cyber-attacks // Computer Security. – 2018. – Vol. 72. – P. 212–233.
10. Menges F., Pernul G. A comparative analysis of incident reporting formats // Computer Security. –2018. – Vol. 73. – P. 87-101.
11. Mavroeidis V., Bromander S. Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence // Proceedings of the 2017 European Intelligence and Security Informatics Conference (EISIC). – Athens, Greece: IEEE, 2017. – P. 91–98.
12. Skopik F. Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks at National Level. – CRC Press: Boca Raton, FL, USA, 2018. – 446 p.
13. Burger E.W., Goodman M.D., Kampanakis P., Zhu K.A. Taxonomy model for cyber threat intelligence information exchange technologies // Proceedings of the ACM Workshop on Information Sharing & Collaborative Security (WISCS). – Scottsdale, AZ, USA, 3 November 2014. – P. 51–60.
14. Asgarli E., Burger E. Semantic ontologies for cyber threat sharing standards // Proceedings of the 2016 IEEE Symposium on Technologies for Homeland Security (HST). – Waltham, MA, USA: IEEE, 2016. – P. 1-6.
15. Serrano O., Dandurand L., Brown S. On the Design of a Cyber Security Data Sharing System // Proceedings of the ACM Workshop on Information Sharing & Collaborative Security (WISCS). – Scottsdale, AZ, USA, 3 November 2014. – P. 61–69.
16. Sullivan C., Burger E. “In the public interest”: The privacy implications of international business-to-business sharing of cyber-threat intelligence // Computer Law & Security Review. – 2017. – Vol. 33, issue 1. – P. 14–29.
17. Zibak A., Simpson A. Cyber threat information sharing: Perceived benefits and barriers // Proceedings of the 14th International Conference on Availability, Reliability and Security. – Canterbury, UK, 26–29 August 2019. – P. 1–9.
18. Wagner C., Dulaunoy A., Wagener G., Iklody A. MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform // Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security. – Vienna, Austria, 24 October 2016. – P. 49-56.
19. Friedman J., Bouchard M. Definitive Guide to Cyber Threat Intelligence. – CyberEdge: Annapolis, MD, USA, 2015. – 72 p.
20. Bryant B., Saiedian H. Improving SIEM Alert Metadata Aggregation with a Novel Kill-Chain Based Classification Model // Computers & Security. – 2020. – Vol. 94. – P. 101817.
21. Shameli-Sendi A., Louafi H., He W., Cheriet M. Dynamic Optimal Countermeasure Selection for Intrusion Response System // IEEE Transactions on Dependable and Secure Computing. – 2018. – Vol. 15, no. 5. – P. 755-770.
22. Farnham G., Leune K. Tools and standards for cyber threat intelligence projects // SANS Institute. – 2013. – Vol. 3., no. 2. – P. 25-31.
23. Schaberreiter T., Kupfersberger V., Rantos K., Spyros A., Papanikolaou A., Ilioudis C., Quirchmayr G. A quantitative evaluation of trust in the quality of cyber threat intelligence sources // Proceedings of the 14th International Conference on Availability, Reliability and Security. – 2019. – P. 1 10.
24. Bianco D.J. The Pyramid of Pain [Jelektronnyj resurs]. – 2013. – URL: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html (data obrashhenija: 05.08.2022).
25. Mokaddem S., Wagener G., Dulaunoy A., Iklody A. Taxonomy driven indicator scoring in MISP threat intelligence platforms [Jelektronnyj resurs]. – 2019. – URL: https://arxiv.org/abs/1902.03914 (data obrashhenija: 05.08.2022).
26. Appala, S.; Cam–Winget, N.; McGrew, D.A.; Verma, J. An actionable threat intelligence system using a publish–subscribe communications model. In Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security, Denver, CO, USA, 12–16 October 2015; pp. 61–70.
27. Wagner, T.D. Cyber Threat Intelligence for “Things”. In Proceedings of the 2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA), Oxford, UK, 3 4 June 2019; pp. 1–2.
28. Menges, F.; Sperl, C.; Pernul, G. Unifying cyber threat intelligence. In Trust, Privacy and Security in Digital Business (TrustBus), Lecture Notes in Computer Science; Springer: Berlin, Germany, 2019; Volume 11711, pp. 161–175.
29. Wagner T.D., Mahbub K., Palomar E., Abdallah A.E. Cyber threat intelligence sharing: Survey and research directions // Computer Security. – 2019. – Vol. 87. – P. 101589
30. Lavrova D.S. An approach to developing the SIEM system for the Internet of Things // Automatic Control and Computer Sciences. – 2016. – Vol. 50. – P. 673-681.
31. Raju B.K., Geethakumari G. Event correlation in cloud: a forensic perspective // Computing. – 2016. – Vol. 98, no. 11. – P. 1203–1224.