ПРОБЛЕМЫ ПРИМЕНЕНИЯ ИНДИКАТОРОВ КОМПРОМЕТАЦИИ ДЛЯ ПРОАКТИВНОГО ПОИСКА УГРОЗ В РАБОТЕ РОБОТОТЕХНИЧЕСКИХ КОМПЛЕКСОВ

Исхаков А.Ю., Мещеряков Р.В., Исхаков С.Ю.

Институт проблем управления им. В.А. Трапезникова РАН,
Россия, г. Москва , ул. Профсоюзная д.65

iay@ipu.ru, mrv@ieee.org, iskhakov.sy@gmail.com

Аннотация: В статье рассмотрены актуальные проблемы применения проактивных алгоритмов детектирования угроз в робототехнических комплексах и структурированы пути их решения. Предложена классификация индикаторов компрометации для проактивного поиска ранее неизвестных угроз в РТК.

Ключевые слова: безопасность, индикатор компрометации, кибератака, робототехнические комплексы.

Введение

Последние изменения в мировом сообществе и стремительный переход к технологиям удаленного доступа привели к тому, что в числе наиболее актуальных объектов кибератак все чаще оказываются телекоммуникационные сети, а также робототехнические и киберфизические системы, формирующие критическую информационную инфраструктуру, которая используется для взаимодействия стратегически важных отраслей экономики.

Применение методов группового управления роботами показало свою эффективность в различных сферах жизни – от бытового применения до промышленных задач и специальных операций. Несмотря на популярность робототехнических комплексов, способных выполнять поставленные задачи с минимальным привлечением человека-оператора, а также повсеместного распространения сетецентрических систем управления, одной из важнейших задач при обеспечении надлежащего уровня защищенности робототехнических групп является автоматизированный мониторинг событий информационной безопасности как центра управления, так и всей инфраструктуры. Целью подобных решений является своевременное оповещение и предупреждение об обнаруженных аномалиях в работе системы, прямо или косвенно являющихся свидетельством инцидента безопасности.

Однако, действительность современной информационной среды обуславливает практически ежедневно меняющийся ландшафт киберугроз, а также техник и тактик действия злоумышленников. Именно поэтому в сфере информационной безопасности сегодня активно формируется тренд на развитие и применение методов и средств защиты информации, позволяющих опережать и предугадывать новые техники злоумышленников. В основе данного тренда лежат алгоритмы и технологии проактивного поиска угроз, позволяющие выявлять ранее неизвестные методы кибератак, которые характерны для высокоавтоматизированных отраслей промышленности, таких как робототехника и киберфизические системы. Среди предпосылок упомянутых трендов можно выделить несколько тезисов.

Во-первых, классические антивирусы не помогают. Конечно, все современные информационные системы проектируются с учетом обязательного использования антивирусной защиты. Особенно объекты критической инфраструктуры. Но классические антивирусы на основе сигнатур и эвристического анализа, как правило не способны выявить бесфайловые атаки и атаки с помощью легитимного ПО. По данным отчета компании Group-IB о расследовании инцидентов за прошлый год, около 85%, компьютеров, вовлеченных в ботнеты, имели антивирусную защиту.

Во-вторых, количество средств защиты в современных стало так велико, что выявляемые ими нарушения составляют большие объемы данных, сложно поддающиеся анализу. Часто на практике наблюдается случаи, когда журналы аудита безопасности так быстро переполняются и затирают данные, что по сути их ведение сводится на нет. Во многих системах отсутствуют механизмы контроял и реагирования на инциденты в круглосуточном режиме, и не уделяется должного внимания анализу лог-файлов, включая сообщения о нейтрализации угроз теми же классическими хостовыми антивирусами.

В данной статье будут рассмотрены и структурированы актуальные проблемы проактивного поиска угроз на примере применения открытых источников индикаторов компрометации при обработке потоков событий в системах управления инцидентами безопасности.

1 Постановка проблемы

1.1 Проблема поиска индикаторов компрометации

Эффективность обнаружения атак на основе применения индикаторов заключается, в первую очередь, в реальной возможности реагировать на выявленную угрозу. Именно поэтому не все индикаторы одинаково полезны при обеспечении защиты объекта, и их значимость необходимо каким-то образом градуировать. В профессиональном сообществе известна модель [2], предложенная исследователем Bianco, характеризующая сложность получения различных типов индикаторов и их ценность в рамках указаннхы ранее ограничений потери данных в событиях безопасности. Модель носит название The Pyramid of Pain и представлена на рисунке 1. Модель отражает взаимосвязь между типами индикаторов компрометации и возможных действий для обнаружения и пресечении действий противника.

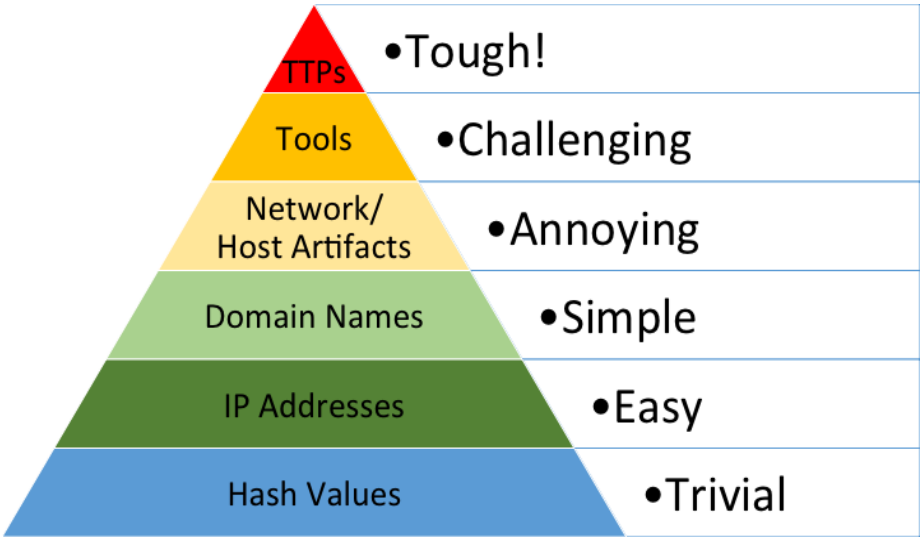

Рис. 1. Модель взаимосвязи индикаторов компрометации, предложенная D. Bianco [2]

Однако, даже если в рамках защищаемой системы будут решены вопросы о потере данных при логировании и определено, какие из индикаторов в данном случае целесообразно добывать и использовать, неизбежно возникает проблему описания этих индикаторов для передачи между объектами защиты. На сегодняшний день существуют различные стандарты идентификаторов компрометации. Среди На слайде представлены наиболее часто используемые на практике.

1. TAXII http://taxii.mitre.org
2. VEDEF http://www.terena.org/activities/tf-csirt/vedef.html
3. CAIF http://www.caif.info
4. DAF http://www.cert-verbund.de/projects/daf.html
5. MANTIS https://github.com/siemens/django-mantis.git
6. RFC 5941 https://tools.ietf.org/html/rfc5941
7. MMDEF http://standards.ieee.org/develop/indconn/icsg/mmdef.html

Поставка актуальных индикаторов компрометации на сегодняшний является отдельной нишей на рынке услуг информационной безопасности. Многие вендоры оказывают услуги по продаже потоков данных об угрозах. При этом каждый из них заявляет различное время актуальности тех или иных типов индикаторов. Также известны и открытые сообщества, представляющие репозитории по обмену такими индикаторами.

1.2 Атрибуция индикаторов компрометации по этапам атаки

Помимо того, какие индикаторы актуальны для выявления инцидентов в защищаемой системе, важно понимать о чем они могут свидетельствовать. То есть не просто обнаружен вирус, а обнаружено вирусное заражение, которое часто применяется в начале распределенной APT-атаке. Для этого необходимо осуществлять моделирование самих атак. Одной из наиболее известных и

первых моделей процесса современных кибератак является модель, предложенная компанией Lockheed Martin [11].

Мы в рамках имеющегося киберполигона проводили моделирования различных атак и постарались отнести типы индикаторов из пирамиды боли с моделью Cyber Kill Chain [1, 10]. При этом старались конкретизировать примеры и представлять даже не типы, а конкретные варианты индикаторов. На рисунке 2 представлены результаты наших наблюдений по результатам регулярно проводимых тестирований и различных исследований внутри лаборатории.

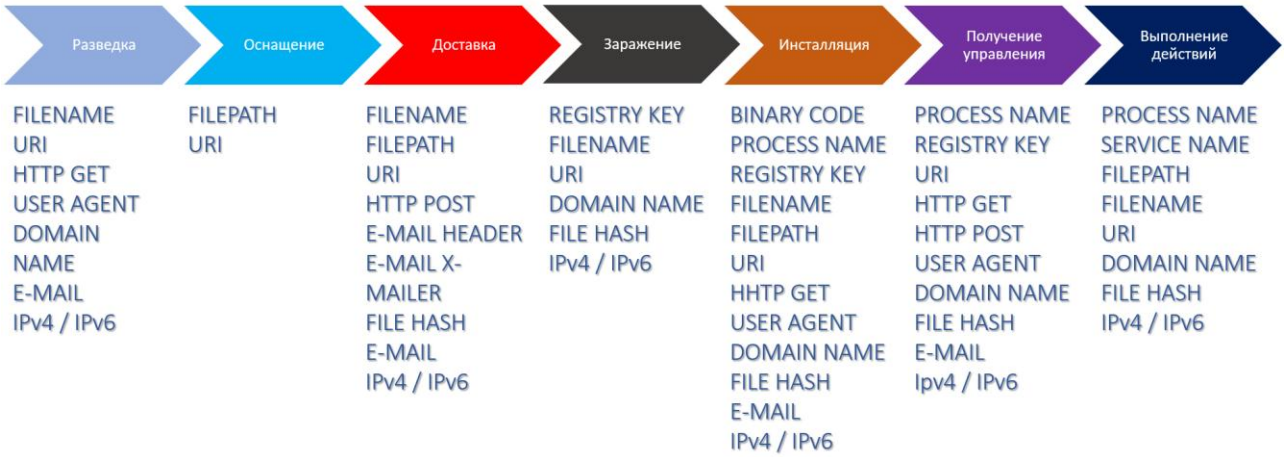

Рис. 2. Атрибуция индикаторов по этапам атаки на основе модели Cyber Kill Chain

2 Классификация индикаторов

Различные технологии оповещения позволяют обнаружить множество подозрительных активностей в работе РТК. Чтобы снизить количество ошибок первого и второго рода, а также избежать дублирования информации, необходимо установить определенные пороговые значения. Если они установлены слишком низко, количество предупреждений будет перегружать аналитиков ложными срабатываниями, что неизбежно приведет к пропускать реальных инцидентов и поставит под угрозу безопасность РТК. Однако, при использовании индикаторов компрометации невозможно полностью избежать ложных срабатываний. Необходимо строить и проверять гипотезы. Существует три варианта результатов проверки гипотезы:

- гипотеза может быть принята и стать случаем реагирования на инцидент
- гипотеза может быть отвергнута, поэтому никаких действий предпринимать не нужно
- гипотеза не может быть ни принята, ни отвергнута, поскольку охотники за угрозами не смогли получить данные, необходимые для принятия обоснованного решения.

Таким образом, можно достичь сокращения разрыва между успешными методами атак и возможностями обнаружения, что сделает охоту за угрозами устаревшей. Различные технологии оповещения обнаруживают множество подозрительных точек данных. В типичной организации имеется множество потенциальных источников оповещения и обогащения данных. Решения класса SOAR позвляют связать их вместе и определить критичность отдельного оповещения, придавая больше контекста путем объединения данных из различных источников. Специалисты по проактивному поиску угроз могут внести значительный вклад в разработку и расширение полуавтоматических программ, обрабатывают действия по обогащению и классификации оповещений.

В ходе исследования различных открытых платформ по обмену индикаторами компрометации мы сформировали классификацию индикаторов, которые можно получать в разрезе операционных систем (рисунок 3). Было проведено исследование в части определения возможности использования открытых источников по обмену индикаторами компрометации для выявления инцидентов в РТК. Согласно исследованию Gartner [4] использование отрктых платформ по обмену индикаторами было отмечено более чем 60% респондентов. Среди достоинств подобных платформ помимо нулевой стоимости можно отметить большое колчиество источников и возомжнгость использования их совместно с платными или собственно сформированными наборами иникаторов. Однако, недостатками их являются много неочевидных нюансов, способствующее малому количеству внедрений. Среди наиболее распространенных индикаторов на исследуемых платформах можно выделить Хостовые, Сетевые и Поведенческие индикаторы.

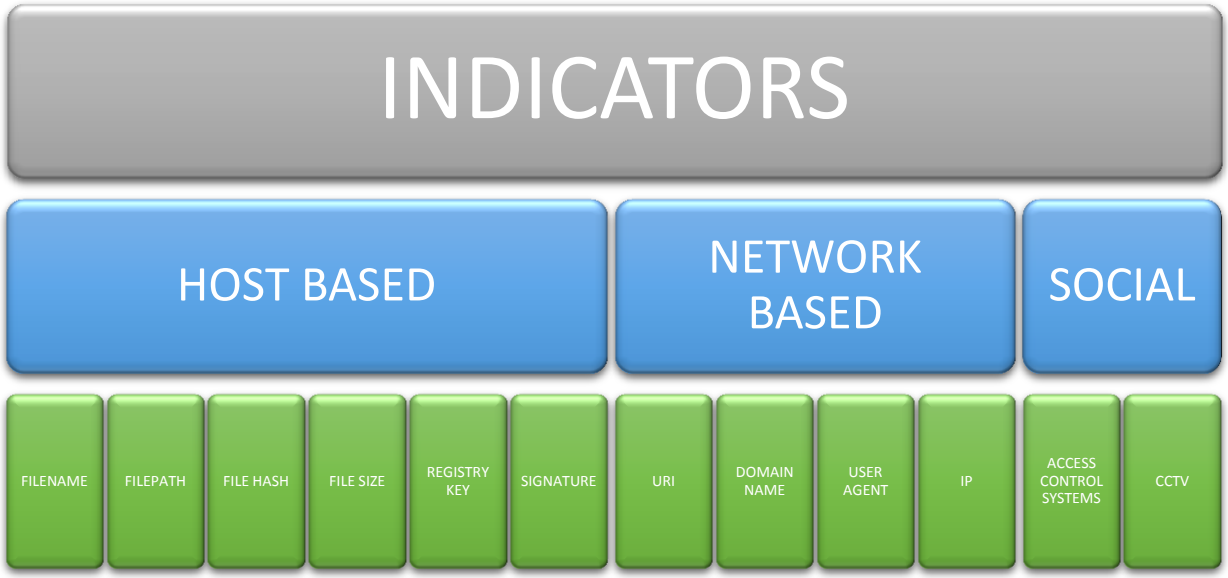

Рис. 3. Предлагаемая классификация индикаторов

В ходе проводимого исследования было обнаружено 130 платформ свободно распространяемых индикаторов, из которых 110 содержали актуальную информацию, т.е. имели обновления в течение последних 6 месяцев. Вышеуказанные платформы содержат индикаторы в следующих форматах.

1. Информация в виде отчетов:

- структурированные (STIX/MISP)
- неструктурированные (pdf/html)

2. Песочницы (json, html)
3. Социальные сети (txt, csv, json, yara, snort).
4. Фиды (txt, csv,json, html)

Опираясь на вышеупомянутую модель The Pyramid of Pain, мы сформировали распределение источников следующим образом (рисунок 4).

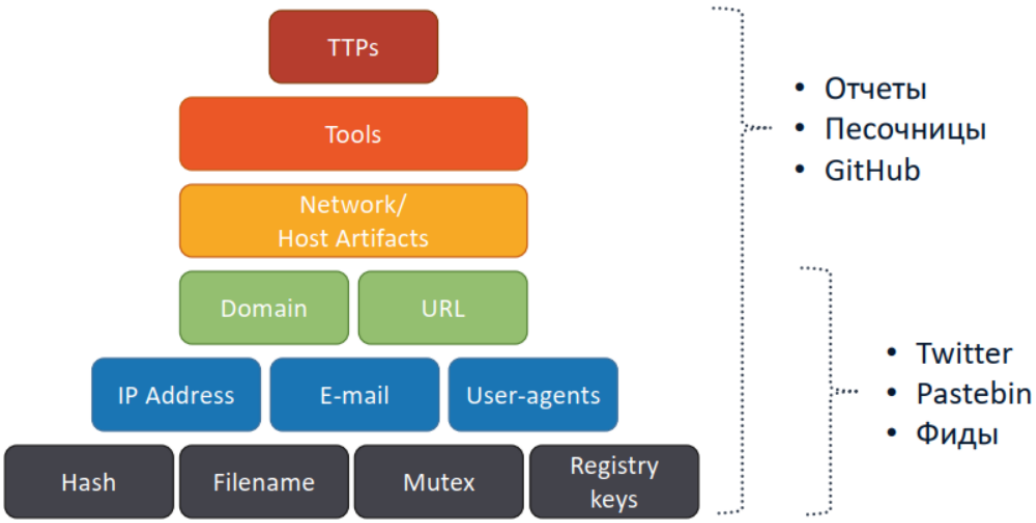

Рис. 4. Распределение источников по типам индикаторов

3 Проведение эксперимента

Для проведения экспериментов использовался кластер из двух нод на платформе Supermicro с двумя процессорами Intel Xeon E5 2.1 ГГц и объемом ОЗУ 128 Гб. Были созданы виртуальные машины на базе различных операционных систем. В качестве активного сетевого оборудования использовались коммутаторы CISCO Catalyst, точки доступа Mikrotik и межсетевой экран CISCO

ASA. Беспроводной сегмент использовался для включения в лабораторную сеть робототехнических комплексов. На рабочих станциях было развернуто специализированное программное обеспечение, позволяющее управлять этими РТК. В качестве объекта применения упомянутых в п.2 источников индикаторов применялся SIEM [6] на базе ArcSight. При этом интенсивность общего потока событий, усредненная по часам за сутки исследования, составила около 800 событий в секунду (events per second, EPS). При этом во время работы с открытыми платформами обмена индикаторами компрометации были выделены следующие проблемы:

1. Подбор источников.
2. Очистка данных.
3. Нормализация индикаторов и контекста.
4. Обогащение.
5. Ранжирование.

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 дублирующихся 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. Кроме того, следует четко понять и сформулировать следующие операции [7]:

- добавление индикатора;
- обновление индикатора;
- удаление индикатора.

При нормализации отчетов могут применяться либо ручной анализ с извлечением значимых индикаторов и помещением их в формат, используемый в защищаемой системе, либо варианты его автоматизации с применением OCR и NLP технологий совместно с ручной валидацией. Наиболее частыми проблемами здесь выступают необходимость ручной валидации результатов, частое применение скриншотов для публикации индикаторов и сложность извлечения информации о связях между индикаторами, в т.ч. для формирования техник и тактик.

Для нормализации данных из социальных сетей наиболее работоспособным механизмом можно определить использование специализированнгых под каждый источник парсеров. Однако, необходимо понимать, что нельзя обойтись только регулярными выражениями. Необходимо представление в какой части текста можно извлечь индикаторы. Немаловажной проблемой являются множественные экранирования и методы автозамены символов при публикации индикаторов в открытых источниках с целью миниминизации случаев резонансного усиления их сипользврания. Кроме того, в подобных ресурсах часто встречаются синтаксические и орфограцически ошибки при формировании индикаторов.

При нормализации фидов возможно использовать унифицированные парсеры для CSV, TSV, Json, plain text. Однако, их применение осложняется частым несоблюдением форматов, соединение в одном источнике несокльких форматов и ошибки в самих индикаторах (рисунок 5).

Рис. 5. Пример ошибок в индикаторах компрометации

В рамках нашего исследования под контекстом понимается описание или название угрозы, которую несет индикатор. Контекст может содержаться в самом отчете, репозитории, публикации в социальнйо сети или фиде, либо в описании на сайте источника. Контекст может включать в себя

название вредоносного программного обеспечения, название группировок атакующих, компаний-жертв или отраслей, где применяется атака. Среди наиболее распространенных проблем можно выделить синтаксические ошибки в названиях, а также синонимы имен Вредоносного программного обеспечения и группировок. Среди данных, обработанных в нашем исследовании к фидам (т.е. источник, предоставляющий индикаторы совместно с описанием угрозы) можно отнести не более 15% платформ.

Перед использованием любого индикатора для выявления инцидентов необходимо понять, можно ли действительно использовать эти ресурсы для реальной атаки. Поэтому не менее важной задачей является очистка индикаторов путем исключения тех из них, которые однозначно приведут к ошибкам первого рода False Positive. Для этой операции стоит использовать аналогичные общедоступные источники, в которых отмечаются публичные ресурсы (публичные dns серверы, наборы хешей и тд). Например:

- RFC 5771, RFC 1918, RFC 6598
- Public DNS, Sinkholes, Malware analysis (VT, shodan, censys, sandboxes)
- NSRL hashsets, NIST Windows Diskprint

Эффективность применения индикаторов на практике можно повысить путем их обогащения, добавив информацию, которая потребуется в расследовании инцидента в первую очередь. Например, можно добавить информацию об ASN, геолокации IP, портах и сервисах, атрибуции облачных провайдеров, точках входа в TOR. В части доменных имен можно использовать информацию из сервисов whois, dns lookup и популряности ресурсов. Применительно к URL можно анализировать код состояния HTTP и принадлежность сертификата HTTPS. Для индикаторов в виде хешей можно подставлять имна файлов и вердикты сервисов проверки, например virustotal.com

При решении задачи обогащения возникает ряд проблем [8]. Во-первых, зачастую нет возможности осуществлять этот процесс в режиме реального времени. Необходимо время и этапы для выявления связей, даже в случаях автоматизации этой задачи. Во-вторых, при использовании сервисов whois нередки случаи неточностей или закрытой информации. В-третьих, некоторые данные, необходимые для обогащения, доступны только на платной основе.

Все эти аспекты необходимо учитывать при проведении обогащения индикаторов, так как основной целью на данном этапе является обогащение именно информацией, актуальной на момент появления индикатора.

Немаловажной задачей является определение значимости индикаторов и оценки их реальной опасности. Для этого необходимо ввести метро, позволяющую 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.

При этом высокий уровень ручных операций при проведении подготовительной работы. Зачастую этот фактор обуславливает возможность проведения такой работы только при наличии болшого штата специалистов, а при отсутствии такового к большому числу ошибок первого рода.

Однако, качество ранжирования [7, 9] очень сильно зависит от собранного конекста и проведенного обогащения, если такое осущствлялось. При этом множество исследований показывают, что нет наиболее преимущественного похода, и зачастую для конкретных случаев примнения индикторов необходимо испробовать несколько методов или их комбинаций. Поэтому, в первую очередь, необходимо выделять минимально возможное множество из доступных наборов индикаторов и производить по ним проверку на общем потоке событий. По остальным индикатором можнго осуществлять ретроспективный поиск, и в случае успешности процесса возможно расширять набор индикаторов для анализа в потоковом режиме.

4 Результаты и обсуждение

Ранее мы обозначили, что одним из важнейших показателей качества индикатора компрометации является его актуальность. Решая данную задачу необходимо периодически удалять устаревшие, утратившие актуальность индикаторы, и передать в СЗИ только необходимые. Механизмы решения этой задачи можно разделить на следующие классы.

1) Соотнесение актуальности индикатороа с уровнем доверия к источнику – платформе, откуда он получен. В данном случае мы предполагаем, что индикатор публикуется источником пока является вредоносным.
2) Задание фиксированног интервала (время жизни), по истечении которого индикатор будет считаться устаревшим и выводиться из обращения.
3) Применение метрик веса и частоты появления по количеству платформ его публикующих, а также по длительности его пристуствия в наборах (с учетом интенсивности обновления с данной платформы).
4) Ручная перепроверка индикатора является наиболее надежным методом с точки зрения практики, однако, такие действия требуют наличия определенного штата специалистов и компетенций, что зачастую недоступно и трудоемко.

Был проведен анализ времени жизни различных типов индикаторов в течение года. При этом наиболее долгое время жизни фиксируется у индикаторов в виде IP-адресов, а наименьшее у URL. Используя подход, основанный на метрике веса и частоте появления с учетом обновления данных, была получена следующая картина по времени жизни индикаторов в зависимости от их опасности (рисунок 6). При этом заметно, что индикаторы с наиболее высокой оценкой опасности устаревают значительно быстрее относительно менее опасных. В первую очередь, это связано с активным ростом интереса профильного сообщества к борьбе с киберугрозами и действиями по их нейтрализации. Кроме того, данная ситуация объясняется стремительностью изменения современного ландшафта атак и принципа их проведения, основанного на внезапности и быстроте действий.

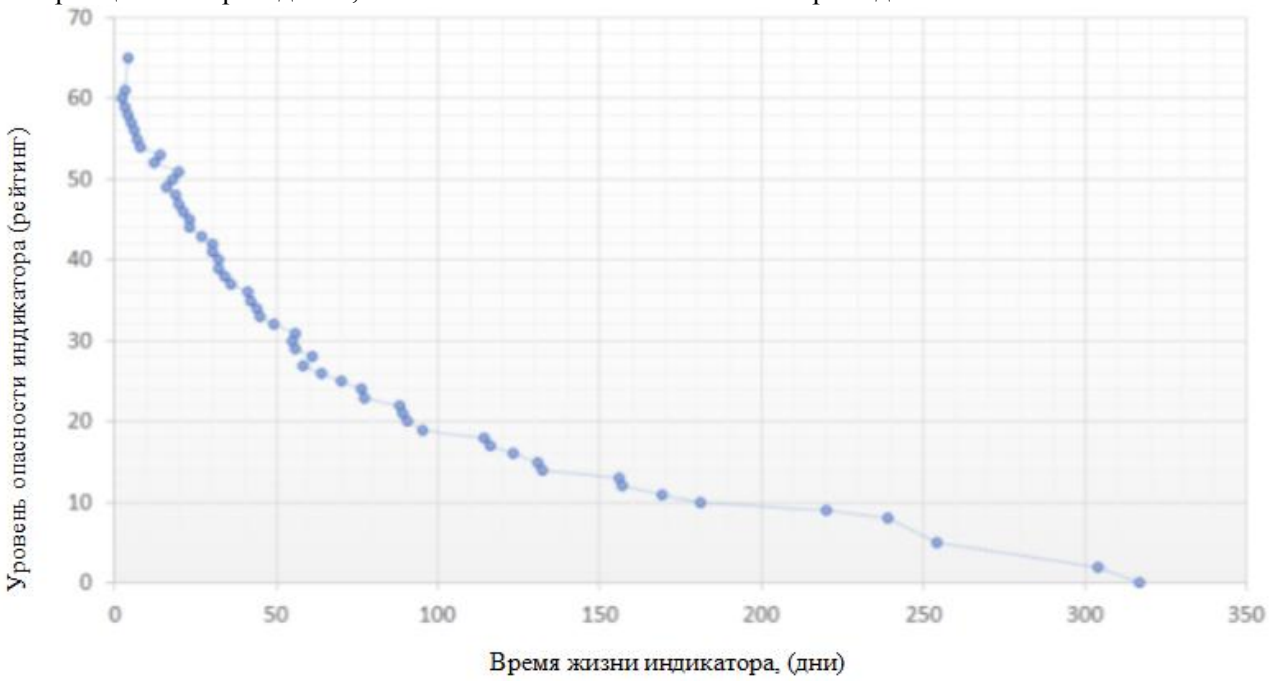

Рис. 6. Устаревание индикаторов по весу и частоте появления

Заключение

Активное внедрение в жизнедеятельность человека различных робототехнических комплексов обусловлено возможностями их интеграции на базе существующей сетевой инфраструктуры как в виде классических сетей передачи данных, так и различных платформ интернета вещей. Помимо очевидного преимущества и получения эффективного инструмента для управления множеством гетерогенных устройств это обстоятельство приводит к наследованию ряда существенных уязвимостей.

Использование индикаторов компрометации является одним из ключевых процессов проактивного поиска угроз для обеспечения защиты РТК. Помимо платных сервисов потоков данных об угрозах существует большое количество отрытых источников. 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. При этом необходимо понимать и делать определенный выбор о том, как будут реализованы упомянутые ранее процессы обработки таких индикаторов

В данной статье труктурированы актуальные проблемы проактивного поиска угроз в работе роботехнических комплексов на примере применения открытых источников индикаторов компрометации при обработке потоков событий в системах управления инцидентами безопасности.

Исследование выполнено при частичной финансовой поддержке РФФИ в рамках научного проекта №19-08-00331.

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. *David J Bianco* “The Pyramid of Pain” http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html
3. *S. Mokaddem, G. Wagener, A. Dulaunoy, A. Iklody,* Taxonomy driven indicator scoring in misp threat intelligence platforms," arXiv preprint arXiv:1902.03914, 2019.
4. 2021 SANS Cyber Threat Intelligence (CTI) Survey https://www.sans.org/reading room/whitepapers/analyst/membership/40080
5. *Lavrova D.* An approach to developing the SIEM system for the Internet of Things // Automatic Control and Computer Sciences. Vol. 50. 2016. – P.673-681.
6. *Raju B.K., Geethakumari G.* Event correlation in cloud: a forensic perspective // Computing. 2016. Vol. 98, № 11. – P.1203–1224.
7. *T. Schaberreiter, V. Kupfersberger, K. Rantos, A. Spyros, A. Papanikolaou, C. Ilioudis, and G. Quirchmayr.* 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.
8. *Han Y., Zhu M., Liu C.* A Service-Oriented Approach to Modeling and Reusing Event Correlations // Proceedings of the IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC). 2018. - P. 498-507.
9. *Shameli-Sendi A., Louafi H., He W., Cheriet M*. Dynamic Optimal Countermeasure Selection for Intrusion Response System // Proceedings of the IEEE Transactions on Dependable and Secure Computing. Vol. 15. 2018, №5, – P. 755-770.
10. *Bryant B., Saiedian H.* Improving SIEM Alert Metadata Aggregation with a Novel Kill-Chain Based Classification Model // Computers & Security, Vol. 94. 2020.
11. *Hoffmann R. Markov* Models of Cyber Kill Chains with Iterations // Proceedings in the 2019 International Conference on Military Communications and Information Systems (ICMCIS). 2019, P. 1-6.