Поиск и скоринг источников индикаторов компрометации по индустриям

Д.А. Туманов, Е.С. Абрамов

Южный федеральный университет, Ростов-на-Дону

Аннотация: В статье авторы предлагают подход, позволяющий провести оценку актуальности использования индикаторов компрометации для определенной индустрии. Выделяются актуальные проблемы, связанные с избыточностью индикаторов компрометации и низким уровнем доверия к их источникам. Предложен подход, позволяющий количественно оценить связи между индикаторами и источником, а также провести скоринг источников.
Ключевые слова: индикатор компрометации, источник индикатора компрометации, рейтинг источников.

Введение

Индикаторы компрометации относятся к киберугрозе как контекстная информация, подтверждающая наличие возможной угрозы или атаки. Когда атака имеет место, она всегда оставляет следы своей деятельности, которые могут быть возможными индикаторами компрометации.

Примеры типичных индикаторов компрометации: сигнатуры вирусов, шаблоны в файлах, нарушения сетевого трафика, или чрезмерное количество запросов на один и тот же файл.

Исследования в области индикаторов компрометации имеют огромное практическое значение, поскольку позволяют выявлять угрозы безопасности информации, а также разрабатывать эффективные меры по защите систем от атак. В данном контексте, использование взвешенных направленных графов как метода представления этих знаний обладает потенциалом для улучшения эффективности анализа и обработки данных, связанных с компрометацией.

Анализ источников показывает, что на сегодняшний день в исследованиях и на практике отсутствует исчерпывающий обзор характеристик и зависимостей общедоступных источников данных по киберугрозам. Научные публикации по представлению и актуализации

индикаторов компрометации рассматривают эту проблему с самых разных сторон.

В работе [1] авторы анализируют технологии анализа угроз и делают акцент на проблеме отсутствия единого мнения о том, как их применять у поставщиков и потребителей данных. В статье также объясняется, почему организации неохотно делятся данными об угрозах. Делается вывод о необходимости стандартизированного представления информации об угрозах для автоматизированного анализа больших объемов данных от источников, которые часто неоднородны и избыточны.

Проблемы оценки качества данных о киберугрозах от источников рассматриваются в работе [2, 3]. Предлагается набор метрики для оценки наборов данных о киберугрозах, относящихся к конкретному инциденту и расширение существующего инструментария анализа индикаторов компрометации и связанных с ними киберугрозах, чтобы сделать оценку качества прозрачной для аналитиков безопасности.

Стандарты представления индикаторов компрометации и связанные с этим проблемы, которые мешают исследователям безопасности использовать их в промышленных секторах рассматриваются в статье [4, 5]. Также обсуждаются потенциальные средства защиты от кибератак. Кроме того, проводится критический анализ существующих работ и доступных инструментов в этой области. Оценивается эффективность используемых индикаторов компрометации, с сопоставлением этих показателей с наиболее часто используемыми целевыми атаками. Наконец, выделяются уроки, которые следует извлечь из литературы, и будущие проблемы в этой области, а также подходы, которые могут быть приняты.

При анализе вышеприведённых источников можно выделить следующую проблему: «Проблема актуализации индикаторов компрометации и их источников в рамках определенной индустрии».

Релевантный поиск индикаторов компрометации

Авторами статьи при выборе источников данных предлагается учитывать индустрию (отрасль) деятельности, т.к специалисты сталкиваются со сложным выбором именно тех источников, которые релевантные защищаемой индустрии рис. 1.

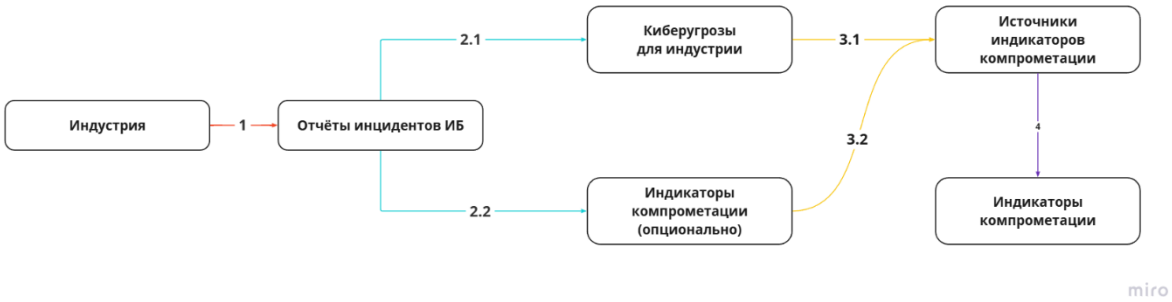

Рис. 1. - Схема первичного поиска индикаторов компрометации

Алгоритм первичного поиска индикаторов компрометации:

1. Обозначить индустрию (отрасль), в рамках которой осуществляется защита информационных процессов и поиск актуальной информации.

2. По обозначенным индустриям осуществляется поиск отчётов различных компаний по инцидентам информационной безопасности (п.1 на рис.1).

3. Из рассмотренных отчетов в рамках рассматриваемых можно выделить типы и описания угроз (п.2.1 на рис.1) и сами индикаторы или их типы (п 2.2 на рис.1).

Обозначенные угрозы и индикаторы (или типы индикаторов) используются для поиска индикаторов компрометации в источниках индикаторов компрометации (п.3.1 - 3.2 и п.4 на рис.1).

Пример использования приведенного алгоритма:

1. Авторы статьи взяли за пример индустрию «Government» (т.е. атаки направлены на правительственные и административные учреждения).

2. Предлагается к рассмотрению отчёт – «APT29 Uses WINELOADER to Target German Political Parties. Prepare for 2024's cybersecurity landscape» [6]. Результат анализа отчёта приведён в таблице №1.

Таблица № 1

Результат анализа отчёта

№ п/п	Индустрии	Угрозы	Типы индикаторов компрометации
1	Government	Wineloader, Envyscout, Burntbatter, Muskybeat, Beatdrop_loader, Password_spray_technique, Donut, Daveshell, Dll_sideloading_technique, Process_injection_technique	Url: 3, File: 16, Hash: 8

3. Для поиска источников воспользуемся платформой с такими источниками OTX AlienVault - Open Threat Exchange и используя полученные данные из отчёта (см. таблицу № 1) найдем источник «Midnight Blizzard Use 'WINELOADER' Malware to Target German Political Parties» [7] индикаторов компрометации. При рассмотрении индикаторов мы видим, что в источнике присутствуют новые индикаторы, которых нет в отчёте [6].

4. Можно также опираться на рассматриваемые в отчёте угрозы при поиске индикаторов компрометации, что позволяет найти еще один «APT29

Uses WINELOADER to Target German Political Parties» [8] и новые типы индикаторов, которых не было в отчёте [6].

Используя предложенный подход, авторы статьи смогли отобрать источники индикаторов компрометации для рассматриваемой отрасли.

Актуализация индикаторов компрометации и скоринг их источников

С течением времени количество наблюдаемых индикаторов компрометации и рассматриваемых источников (далее «фид(-ы)») растёт (см. рис. 2).

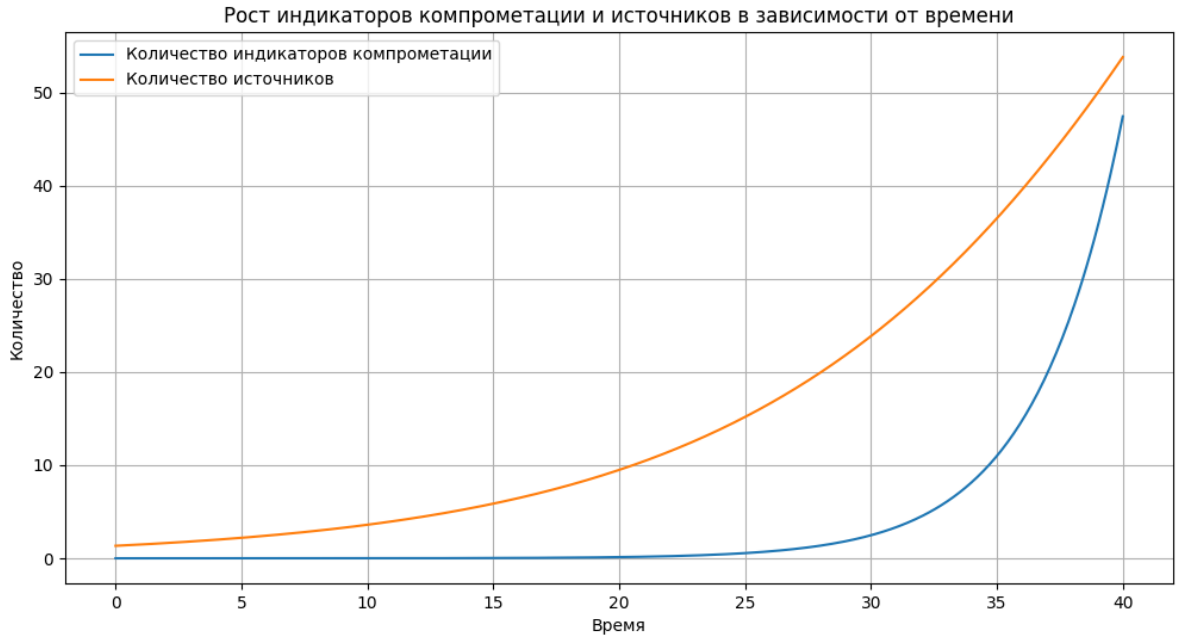

Рис. 2. – Рост количества индикаторов компрометации и фидов в зависимости от времени

На рис. 2 видно, что в начале количество индикаторов увеличивается, а количество фидов нет. Причина этому в том, что некоторые индикаторы были получены из отчёта [6] и использовались при поиске фидов.

Авторы статьи во введении как раз указывали на эту проблему и предлагали решать её актуализацией связи между индикатором компрометации и фидом - формула (1).

$$W = \left(\frac{T-\Delta T}{T}\right) \times (e^{-wT \times \Delta T}) \times wt \times wf \times (1 - e^{-ws}), \quad (1)$$

где W – вес связи ; T – время жизни индикатора компрометации, зависит от типа индикатора компрометации; ΔT– разница во времени между первым появлением и проверкой индикатора компрометации в информационной системе (например, в SIEM); wT – скорость затухания и индикатора компрометации – от 0 до 1; wt – коэффициент актуальности связанной угрозы – от 0 до 1; wf – коэффициент уровня доверия к источнику индикатора – от 0 до 1; ws – частота обнаружения индикатора компрометации в информационной системе.

Экспонента используется в формуле (1) для моделирования определённого типа поведения или зависимости, который сложно описать линейными отношениями. В приведённых исследованиях авторы статьи работают с процессами, которые растут или уменьшаются с постоянной скоростью.

Веса этих связей оказывают влияние на скоринг источников. Таким образом, чтобы получить общий скоринг источника, нужно рассчитать W_i для каждого индикатора, связанного с источником, используя формулу (1) веса связи и суммировать все рассчитанные веса по формуле (2) и так мы можем получить общий рейтинг фидов для определённой индустрии:

$$Sf = \sum_{i=1}^{N} W_i, \quad (2)$$

где Sf – значение скоринга для фида; $\sum_{i=1}^{N} W_i$ – сумма весов рёбер со связанными индикаторами компрометации.

Приведём пример на полученных ранее данных (см. таблицу №2).

Таблица № 2

Данные для расчёта весов рассматриваемых индикаторов

№ п/п	Индикатор	Тип	T	ΔT	wT	wt	wf_1	wf_2	ws
1	IOC1	domain	30	5	0.05	0.7	0.6	-	10
2	IOC2	domain	30	10	0.05	0.7	0.6	-	20
3	IOC3	url	45	15	0.04	0.7	-	0.5	15
4	IOC4	url	45	20	0.04	0.7	-	0.5	25
5	IOC5	md5	60	30	0.03	0.7	0.6	0.5	30
6	IOC6	md5	60	25	0.03	0.7	0.6	0.5	6

Из таблицы №2 видно, что индикаторы IOC5, IOC6 связаны с двумя источниками. Связи будут рассчитаны для двух источников и использоваться при скоринге. При этом рассматриваются не все найденные индикаторы компрометации и угрозы из таблицы №1 для более удобной наглядности. Применим формулу (1) и (2), отобразим результаты в виде взвешенного комбинированного графа (см. рис. 3).

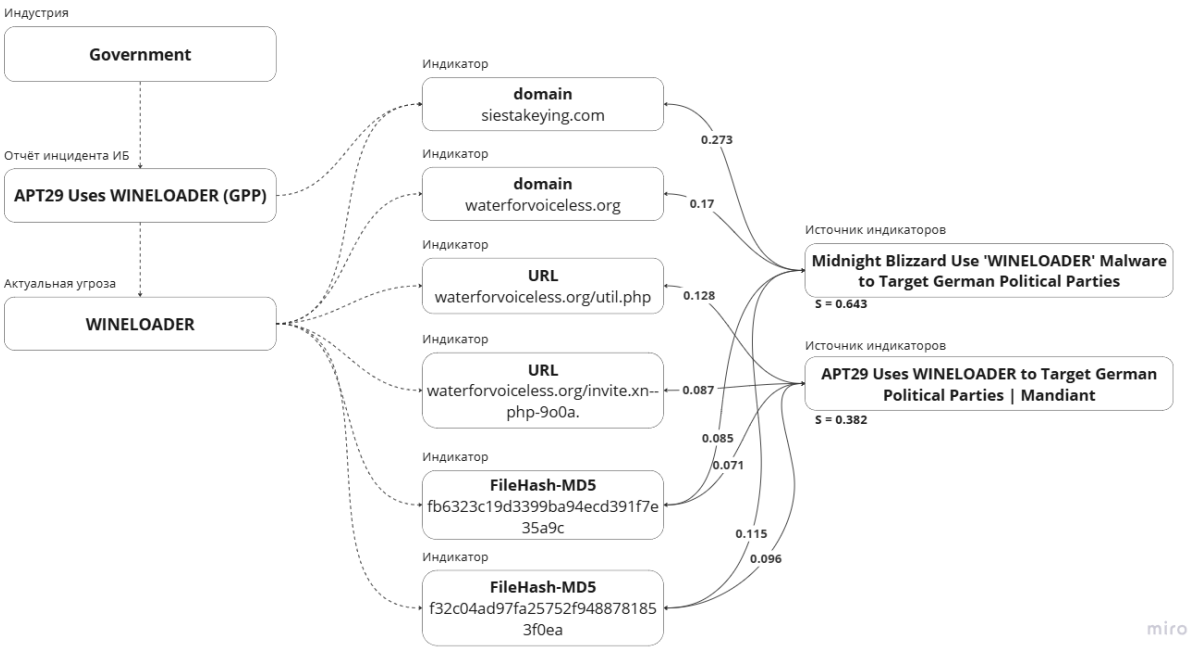

Рис. 3. - Данные, полученные при анализе источников

На рис.3 количественно и наглядно оценены связи между индикаторами компрометации и фидами, тем самым авторы статьи показывают актуальность не только индикатора, но и фида. В итоге мы получим перечень фидов с рейтингом для определённой индустрии. Тем самым мы можем актуализовать список используемых источников. Для обмена данными о киберугрозах и в данном случае индикаторов компрометации используются стандарты STIX 2.1 [9] и TAXII [10].


```
{
  "id": "bundle--351cf827-f0bb-4519-aad4-4cc279613776",
  "spec_version": "2.1",
  "objects": [
    ...
    {
      "type": "indicator",
      "id": "indicator--fb7d8b82-c618-4ad0-b132-8bf6ca84884c",
      "created": "2024-05-01T12:34:56.789Z",
      "modified": "2024-05-01T12:34:56.789Z",
      "pattern": "[domain-name:value = 'waterforvoiceless.org']",
      "pattern_type": "stix",
      "valid_from": "2023-10-01T12:00:00Z"
    },
    ...
    {
      "type": "feed",
      "id": "feed--8e8878a0-3852-4f8c-944e-b00685d3789c",
      "created": "2024-05-01T12:34:56.789Z",
      "modified": "2024-05-01T12:34:56.789Z",
      "name": "Midnight Blizzard Use 'WINELOADER' Malware to Target German Political Parties",
      "link": "https://otx.alienvault.com/pulse/65ff4c249cf88cc0b3e068dd",
      "scoring": 0.643,
      "pattern_type": "stix",
      "valid_from": "2023-10-01T12:00:00Z"
    },
    ...
    {
      "type": "relationship",
      "id": "relationship--1716a873-8f65-41c4-8884-b63156ec80c4",
      "created": "2023-10-01T12:34:56.789Z",
      "modified": "2023-10-01T12:34:56.789Z",
      "relationship_type": "based-on",
      "source_ref": "indicator--fb7d8b82-c618-4ad0-b132-8bf6ca84884c",
      "target_ref": "feed--8e8878a0-3852-4f8c-944e-b00685d3789c",
      "weight": 0.17
    },
    ...
  ]
}
```


Рис. 4. - Пример бандла данных в стандарте STIX 2.1

На рис. 4 приведен фрагмент такого «бандла». Виден индикатор компрометации, связанный с ним источник и приведена информация об этой связи. Важно отметить, что тип данных объекта «feed» и вес связи («relationship») в стандарте отсутствует. Авторы статьи расширяют стандарт, не нарушая согласованности данных при их обмене.

Заключение

В ходе работы был предложен набор метрик для оценки качества наборов данных об индикаторах компрометации, что позволяет более объективно и структурировано подходить к проблеме выявления и анализа индикаторов компрометации и оценке их источников.

Авторы предложили методику, основанную на использовании взвешенных комбинированных графов для представления и анализа индикаторов компрометации. Важно отметить, что предложенная методика также облегчает процесс оценки качества используемых источников индикаторов компрометации, повышая прозрачность и доверие к данным среди аналитиков безопасности.

Далее авторы планируют глубже рассмотреть наборы различных метрик и зависимости, которые влияют на их значения, а также интегрировать предложенную методику в платформы для анализа индикаторов компрометации.

Литература

1. Wiem Tounsi, Helmi Rais, A survey on technical threat intelligence in the age of sophisticated cyber-attacks. Computers & Security. Volume 72. 2018. pp. 212-233. URL: doi.org/10.1016/j.cose.2017.09.001.

2. Schlette, D., Böhm, F., Caselli, M. et al. Measuring and visualizing cyber threat intelligence quality. Int. J. Inf. Secur. 20. 2021. pp. 21–38. URL: doi.org/10.1007/s10207-020-00490-y.

3. Абрамов Е.С., Тарасов Я.В. Применение комбинированного нейросетевого метода для обнаружения низкоинтенсивных DDoS-атак на web-сервисы // Инженерный вестник Дона. 2017. №3. URL: ivdon.ru/ru/magazine/archive/N3y2017/4354.

4. Менциев А.У., Пахаев Х.Х., Айгумов Т.Г. Угрозы безопасности узкополосного интернета вещей и меры противодействия // Инженерный вестник Дона. 2021. №10. URL: ivdon.ru/ru/magazine/archive/N3y2019/5801.

5. Asiri M.Saxena N.Gjomemo R.Burnap P.See. Understanding Indicators of Compromise against Cyber-attacks in Industrial Control Systems: A Security Perspective. ACM Transactions on Cyber-Physical Systems (2023) URL: dl.acm.org/doi/10.1145/3587255.

6. Jenkins L., Black D., APT29 Uses WINELOADER to Target German Political Parties. Prepare for 2024's cybersecurity landscape. URL: mandiant.com/resources/blog/apt29-wineloader-german-political-parties.

7. OTX AlienVault - Open Threat Exchange. Midnight Blizzard Use 'WINELOADER' Malware to Target German Political Parties. URL: otx.alienvault.com/pulse/65ff4c249cf88cc0b3e068dd.

8. OTX AlienVault - Open Threat Exchange. APT29 Uses WINELOADER to Target German Political Parties. URL: otx.alienvault.com/pulse/6601491afe42a49da1036107.

9. STIX Version 2.1. 2021. URL: docs.oasis-open.org/cti/stix/v2.1/cs01/stix-v2.1-cs01.html.

10. Trusted Automated Exchange of Intelligence Information (TAXII) Version 2.1. 2021. URL: oasis-open.github.io/cti-documentation/resources.html#taxii-21-specification.

References

1. Wiem Tounsi, Helmi Rais Computers & Security. Volume 72. 2018. pp. 212-233. URL: doi.org/10.1016/j.cose.2017.09.001.

2. Schlette, D., Böhm, F., Caselli, M. et al. Measuring and visualizing cyber threat intelligence quality. Int. J. Inf. Secur. 20. 2021. pp. 21–38. URL: doi.org/10.1007/s10207-020-00490-y.

3. Abramov E.S., Tarasov Ya.V. Inzhenernyj vestnik Dona. №3. URL: ivdon.ru/ru/magazine/archive/N3y2017/4354.

4. Menciev A.U., Pahaev H.H., Ajgumov T.G. Inzhenernyj vestnik Dona. 2021. №10. URL: ivdon.ru/ru/magazine/archive/N3y2019/5801.

5. Asiri M.Saxena N.Gjomemo R.Burnap P.See. Understanding Indicators of Compromise against Cyber-attacks in Industrial Control Systems: A Security Perspective. ACM Transactions on Cyber-Physical Systems (2023) URL: dl.acm.org/doi/10.1145/3587255

6. Jenkins L., Black D., APT29 Uses WINELOADER to Target German Political Parties. Prepare for 2024's cybersecurity landscape. URL: mandiant.com/resources/blog/apt29-wineloader-german-political-parties.

7. OTX AlienVault - Open Threat Exchange. Midnight Blizzard Use 'WINELOADER' Malware to Target German Political Parties. URL: otx.alienvault.com/pulse/65ff4c249cf88cc0b3e068dd

8. OTX AlienVault - Open Threat Exchange. APT29 Uses WINELOADER to Target German Political Parties. URL: otx.alienvault.com/pulse/6601491afe42a49da1036107.

9. STIX Version 2.1. 2021. URL: docs.oasis-open.org/cti/stix/v2.1/cs01/stix-v2.1-cs01.html.

10. Trusted Automated Exchange of Intelligence Information (TAXII) Version 2.1. 2021. URL: oasis-open.github.io/cti-documentation/resources.html#taxii-21-specification.

Дата поступления: 30.06.2024

Дата публикации: 8.08.2024