УДК 004.023

Использование фидов

В. М. Картак[1], Н. М. Башмаков[2]

[1] KVmail@mail.ru, [2] nail.bashmakov@gmail.com

ФГБОУ ВО «Уфимский университет науки и технологий» (УУНиТ)
Институт физики молекул и кристаллов УФИЦ РАН, Россия

Аннотация. В статье рассматривается такое направление в информационной безопасности как разведка кибер-угроз. Анализируется использование таких индикаторов компрометации как *ip*-адреса, полученных из свободно распространяемых фидов. Фиды сгруппированы по типам отслеживаемой вредоносной активности. Выдвинута гипотеза о большей эффективности применения для конкретной инфраструктуры актуального для нее набора фидов. Проведен вычислительный эксперимент, подтверждающий гипотезу.

Ключевые слова: разведка кибер-угроз, фиды, индикаторы компрометации.

ВВЕДЕНИЕ

По мере продолжающейся цифровизации человечества компьютерные атаки стали серьезной угрозой для нормального функционирования различных информационных систем. Большой популярностью пользуются атаки вирусов-шифровальщиков, в ходе которых злоумышленники шифруют данные и требуют выкуп для возвращения доступа к ним. Более того, компьютерные атаки уже вышли за пределы исключительно информационных систем, примером чего может служить атака на нефтяную компанию *«Colonial Pipeline»* в 2021 году [1] результатом которой стал дефицит нефтепродуктов в Техасе. Совершенно закономерным является и внимание к проблеме, в том числе на самом высоком уровне, уровне глав государств [2].

Времена энтузиастов-романтиков и шутников прошли, так что основным мотивом современных взломщиков является жажда наживы. Для того, чтобы оставаться эффективными хакеры вынуждены совершенствовать свой инструментарий, объединяться в группы, повышать свою квалификацию. Профессиональные и группы хакеров обычно именуют *APT*-группами. Первоначально данный термин применялся для описания взломщиков, которым приписывалось сотрудничество с какими-либо государствами и проведение акций в интересах их правительств. Часто такие группы атакуют различные государственные структуры, научно-исследовательские институты, в попытках украсть информацию или технологии. Позднее термин *APT*-группа стали применять и к просто высококвалифицированным хакерам. В целом сформировался целый теневой рынок, на котором продаются неизвестные ранее эксплойты, доступы к уже взломанным организациям, вредоносное ПО, оказываются услуги по обфускации полезной нагрузки. Там же размещаются заказы и принимаются заказы на взлом. Общая тенденция – переход от массовых атак начала века к сложным целевым атакам [3].

ФИДЫ

Специалисты информационной безопасности стараются соответствовать и принимать меры, чтобы дать адекватный и эффективный ответ вызовам времени. Развиваются ставшие уже классическими средства защиты – антивирусы, межсетевые экраны, системы обнаружения вторжений. Появляются и развиваются новые классы решений, возникают новые направления, призванные дать возможность эффективнее противодействовать злоумышленникам. Одним из таких направлений является разведка кибер-угроз, *threat intelligence*.

В целом это направление можно охарактеризовать как сбор и использование информации о конкретных актуальных угрозах безопасности, индикаторах компрометации, соответствующих данной угрозе, последствиях реализации угрозы, рекомендации по предотвращению или ликвидации последствий [4].

Индикатор компрометации – это некий признак в инфраструктуре, указывающий на возможную нежелательную, вредоносную активность [5]. Такие индикаторы компрометации могут объединяться в списки, которые называют фидами. К основным типам индикаторов, которые группируют в фиды можно отнести *ip*-адреса, доменные имена, *url*-ссылки, хэши файлов.

Фиды могут составляться как крупными компаниями, основным направлением деятельности которых является информационная безопасность, так и группами энтузиастов, даже одиночками, исследователями, сообществами. Фиды от компаний обычно предлагаются за плату, в то время как фиды от сообщества часто распространяются свободно.

Свободно распространяемые фиды могут составляться автоматизированным образом, на основе работы сети ловушек-*honeypot*. Такое разнообразие источников фидов приводит к такому же разнообразию их качества – в фидах могут появляться записи об индикаторах, которые на самом деле никакой вредоносной активности не проявляли, так называемые *false positive*.

Выделяют 4 сценария использования фидов: превентивное блокирование, детектирование, ретроспективный анализ и расследование [5]. Учитывая, что даже в фидах от крупных компаний могут встречаться ошибки [6], а также порой значительную их цену пользуются и свободно распространяемыми фидами. При этом возникает несколько проблем. При реализации сценария превентивного блокирования могут быть заблокированы ресурсы, необходимые для осуществления бизнес-процессов, что приведет к их простою. В сценарии детектирования не должно быть большого числа ложных срабатываний, поскольку это может привести к излишней нагрузке на аналитика или администратора. Так же может существовать ограничение на количество индикаторов компрометации, которое может использоваться в сценариях детектирования и блокирования, исходящее из ограничений программных и аппаратных средств. Следовательно, должен осуществляться подбор фидов для конкретной инфраструктуры и исходя из используемого сценария.

Кроме этого, следует учитывать, что такие индикаторы компрометации как *ip*-адерса и доменные имена часто проявляют вредоносную активность лишь краткий момент времени, после чего злоумышленники перемещаются на другую инфраструктуру. Происходит это как раз для того, чтобы снизить эффективность обмена информацией об индикаторах компрометации. Следовательно *ip*-адреса и доменные имена, попавшие в фиды остаются актуальными лишь небольшой промежуток времени.

Для решения проблемы со ставшими не актуальными индикаторами компрометации разработчиками платформы *MISP* был предложен метод, который основывался на постепенном уменьшении оценки индикатора с течением времени [7]. А, например, в работе исследователей из Амстердама исследуются способы снижения количества *false* positive индикаторов [8].

РЕЗУЛЬТАТЫ

Для проведения эксперимента было выбрано 44 фида, содержавших *ip*-адреса. Фиды имели различную периодичность обновления индикаторов в них, мы же загружали в нашу базу данных индикаторы компрометации раз в сутки. Проанализировав фиды, мы заметили, что они различаются по типам отслеживаемой вредоносной активности. После этого мы сгруппировали их по этим типам (см. табл. 1). Была выдвинута гипотеза, что для определенной инфраструктуры следует использовать только индикаторы компрометации из фидов, отслеживающих актуальную и признанную нежелательной активность.

Таблица 1.

Группы фидов по типам

Группа фидов	Фиды
Bots – списки *Command & Control* серверов ботнетов	*feodotracker, sslipblacklist, mirai, blocklist_bots, botscout_1d*
Bruteforce – атаки перебором паролей	*dataplane_vncrfb, dataplane_sshpwauth, blocklist_ssh*
Iptelephony – атаки на *ip*-телефонию	*dataplane_sipregistration, dataplane_sipquery, dataplane_sipinvitation, blocklist_sip, blocklist_asterisk*
General – фиды, общей направленности, или для которых не удалось определить специфику	*ipspamlist, malsilo, benkow_general, rstcloud, alienvault, emergingthreats, firehol_level1, ci-badguys, greensnow, cybercure, emergingthreats, blocklist_all, threatcrowd*
Phishing – фишинговые рассылки	*Phishstats*
Mail – атаки электронной почты	*pop3gropers, blocklist_email, blocklist_imap, blocklist_pop3, blocklist_postfix*
FTP – атаки на *FTP*	*blocklist_ftp, blocklist_proftpd*
Web – атаки на веб-ресурсы	*blocklist_apache, cruzit_web_attacks*
Miners – индикаторы, связанные с майнингом криптовалюты	*bitcoin_nodes_1d*
Anonymizers – индикаторы связанные с сервисами анонимизации	*socks_proxy_7d, sslproxies_1d, secureupdates*

Проверить эффективность использования фидов было решено в двух тестовых инфраструктурах: инфраструктура 1 представляла собой веб-сервер, инфраструктура 2 – службу вебинаров, трафик к которой анализировался системой обнаружения вторжений (СОВ). Из журналов веб-сервера были выделены *ip*-адреса, с которых были осуществлены неудачные попытки авторизоваться, из журналов СОВ – зафиксированные попытки осуществить эксплуатацию уязвимости. Журналы веб-сервера анализировались за весь период его работы – несколько лет, журналы СОВ за последний месяц (январь 2022).

ЭКСПЕРИМЕНТ

После этого из всего набора индикаторов компрометации из всех фидов сформировали наборы в 10000 и 100000 наиболее актуальных *ip*-адресов и осуществили поиск пересечений между сформированными наборами и наборами *ip*-адресов, атаковавших наши инфраструктуры 1 и 2.

Поскольку обе наши инфраструктуры представляли собой веб-сервисы, мы сделали предположение, что для них являются актуальными индикаторы из фидов с типами *web* и *general*. После чего повторили эксперимент.

Затем мы заметили, что большая часть индикаторов компрометации в обоих наборах поступила из фида *rst_cloud*, который оказался самым объемным. Тогда было принято решение повторить эксперименты исключив этот фид из рассмотрения. Результаты экспериментов приведены в табл. 2.

Таблица 2.

Результаты экспериментов

Количество индикаторов компрометации	10000		100000	
Инфраструктура	Веб-сервер	Вебинары+СОВ	Веб-сервер	Вебинары+СОВ
Все фиды	0(0.0%)	1(0.52%)	22(0.87%)	37(19.07%)
Только актуальные	0(0.0%)	1(0.52%)	47(1.86%)	47(24.23%)
Все фиды без rst_cloud	11(0.44%)	2(1.03%)	67(2.65%)	45(23.2%)
Только актуальные без *rst_cloud*	0(0.0%)	2(1.03%)	116(4.59%)	93(47.94%)

ЗАКЛЮЧЕНИЕ

В данной работе рассматривалось применение свободно распространяемых фидов – списков индикаторов компрометации. Индикаторы компрометации могут использоваться для обнаружения нежелательной активности в инфраструктуре или для превентивного блокирования взаимодействия с подозрительными ресурсами. В любом из сценариев использования могут возникают проблемы. Например, технические ограничения средств защиты информации, приводящие к невозможности использовать весь массив индикаторов компрометации, который может исчисляться сотнями тысяч и миллионами сущностей. Еще одной проблемой является наличие ложно позитивных индикаторов.

Атаки на сервис для проведения вебинаров фиксировались в тот же период, в который осуществлялся сбор данных из фидов, в отличии от журналов веб-сервера - список *ip*-адресов атаковавших его был сформирован за несколько лет работы сервера, причем за 2021-2022 годы количество атак было незначительным. Это позволяет сделать вывод о том, что фиды в значительной степени соответствуют актуальным *ip*-адресам, используемым злоумышленниками.

Получившиеся результаты, свидетельствуют о том, что отобранный набор фидов в гораздо большей степени подходит для инфраструктуры, в которой расположен сервис для вебинаров. Так же можно сделать вывод, что в целом предположение о необходимости отбирать только актуальные для конкретной инфраструктуры индикаторы компрометации нашло свое подтверждение.

СПИСОК ЛИТЕРАТУРЫ

1. Романовский Георгий Борисович (2021). ПРАВО, ОБЩЕСТВО, ГОСУДАРСТВО В ЭПОХУ РАЗВИТИЯ ГЛОБАЛЬНЫХ УГРОЗ. Наука. Общество. Государство, 9 (2 (34)), 59-67.
2. Шакиров О. Киберсаммит Путина и Байдена [Электронный ресурс]. — Режим доступа: https://russiancouncil.ru/analytics-and-comments/analytics/kibersammit-putina-i-baydena/
3. Friedman J. Definitive Guide to Cyber Threat Intelligence, J. Friedman, M. Bouchard. - 2015.
4. Новиков А. Threat Intelligence: куда и как его «прикладывать» / А. Новиков // Журнал "Information Security/ Информационная безопасность" – 2020. – 6. - 38-39.
5. Сергеев Ю. Особенности сбора, агрегации и ранжирования индикаторов компрометации / Ю. Сергеев // Журнал "Information Security/ Информационная безопасность" – 2020. – 5. - 22-23.
6. Пирожков А. Фиды для SOC. Осведомлен – значит вооружен/ А. Пирожков // Журнал "Information Security/ Информационная безопасность" – 2020. – 5. - 24-25.
7. Iklody A. Decaying Indicators of Compromise / A. Iklody, G. Wagener, A. Dulaunoy, S. Mokaddem. // 2018.
8. Ermerins J. Scoring model for IoCs by combining open intelligence feeds to reduce false positives / J. Ermerins, N.van Noort L. Velasco // 2020.

ОБ АВТОРАХ

БАШМАКОВ Наиль Маратович, аспирант 1-го года обучения ФИРТ.
КАРТАК Вадим Михаилович, доктор ф-м наук, зав. каф. ВТиЗИ ФИРТ.

METADATA

Title: Usage of feeds
Affiliation: Ufa University of Science and Technology (UUST), Russia.
Email: [2] nail.bashmakov@gmail.com [1], KVmail@mail.ru
Language: Russian.
Source: Molodezhnyj Vestnik UGATU (scientific journal of Ufa University of Science and Technology), no. 1 (23), pp. 22-25, 2023. ISSN 2225-9309 (Print).
Abstract:
Key words: cyber threat intelligence, feeds, indicators of compromise.
About authors: This article is discussing such direction in information security as intelligence of cyber threats. The use of such indicators of compromise as ip-addresses obtained from freely distributed feeds is analyzed. The feeds are grouped by the type of malicious activity being tracked. A hypothesis has been put forward about the greater efficiency of using the set of feeds that is relevant for a specific infrastructure. A computational experiment confirming the hypothesis was carried out.
BASHMAKOV, Nail Maratovich, postgraduate student 1 year, Ufa state aviation technical University.
KARTAK, Vadim Mihailovich, assistant Professor, Ufa state aviation technical University.
ussia