16. *Pobegaylov O.A., Kravchenko I.V., Kozhukhovskiy S.O.* Mobil'nye roboty vertikal'nogo peremeshcheniya [Mobile robots of vertical movement], *Inzhenernyy vestnik Dona* [Engineering Bulletin of the Don], 2010, No. 4 (14), pp. 85-95.
17. *Nansai Shunsuke & Mohan Rajesh Elara.* A Survey of Wall Climbing Robots: Recent Advances and Challenges, *Robotics,* 2016, 5. 14. 10.3390/robotics5030014.
18. *Unver O. & Uneri Ali & Aydemir Alper & Sitti M.* Geckobot: A gecko inspired climbing robot using elastomer adhesives, *Proceedings - IEEE International Conference on Robotics and Automation,* 2006, pp. 2329-2335. 10.1109/ROBOT.2006.1642050.
19. *Khachatryan A.A., Briskin E.S.* O peremeshchenii mobil'nogo robota po proizvol'no orientirovannym poverkhnostyam [On the movement of a mobile robot on arbitrarily oriented surfaces], *Izvestiya VolgGTU* [Bulletin of the Volgograd State Technical University], 2022, No. 9 (268), pp. 86-93.
20. *Khachatryan A.A., Smirnaya L.D.* Osobennosti dinamiki upravlyaemogo dvizheniya robota, opirayushchegosya na razlichno orientirovannye rovnye poverkhnosti [Features of the dynamics of controlled motion of a robot resting on differently oriented flat surfaces], *Izvestiya VolgGTU* [Bulletin of the Volgograd State Technical University], 2024, No. 4 (287), pp. 84-87.

Хачатрян Арам Араи – Волгоградский государственный технический университет; e-mail: Aram-081097@mail.ru; г. Волгоград, Россия; тел.: +79375508766; кафедра «Динамика и прочность машин»; аспирант.

Брискин Евгений Самуилович – e-mail: dtm@vstu.ru; тел.: +78442248113; кафедра «Динамика и прочность машин»; д.ф.-м.н.; профессор.

Khachatryan Aram Arai – Volgograd State Technical University; e-mail: Aram-081097@mail.ru; Volgograd, Russia; phone: +79375508766; the Department of "Dynamics and strength of machines"; postgraduate student.

Briskin Evgeny Samuilovich – e-mail: dtm@vstu.ru; phone: +78442248113; the Department of "Dynamics and strength of machines"; dr. of phys. and math. sc.; professor.

УДК 004.056 DOI 10.18522/2311-3103-2024-6-209-218

С.А. Смирнов, Н.Ю. Паротькин, В.В. Золотарев

АВТОМАТИЗАЦИЯ ИСПОЛЬЗОВАНИЯ ЛОЖНЫХ КОМПОНЕНТОВ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

Рассматривается вопрос применимости ложных информационных систем и их компонентов в построении автоматизированной системы развертывания прикладной реализации технологии ложных компонентов и управления ею – для совершенствования системы предупреждения атак. Приводятся основные преимущества технологии и роль в стратегии информационной безопасности, задающие специфику и область практического применения ее средств и инструментов. Рассматриваются основы архитектуры и особенности применения технологии, а также ее ограничения. Указываются цель и назначение использования современной технологии в разрезе раскрытия ключевых принципов ее реализации. Кроме того, были проанализированы нормативно-правовые публикации и иные рекомендации, составляющие лучшие практики в области её использования. Рассмотрены концепция и архитектура итогового автоматизированного решения в интеграции в информационные системы и системы защиты, описано функциональное содержание итогового решения. Отличительной особенностью предлагаемого решения является использование управляемых механизмов контейнеризации, обеспечивающих широкие возможности по масштабированию решения и изоляции скомпрометированных компонентов системы в результате действий злоумышленника. Схематически отражается сформулированный процесс практического исполнения системы автоматизации в перспективе подсистем решения и в отношении к зависимым компонентам (предлагаемым документам, внешним средствам и системам) и условиям протекания составляющих операций. Также приводится модель развертывания и функционирования распределенной системы автоматизации в последовательности: настройка сервера развертывания (включая обеспечение), развертывание сети ложных компонентов-ловушек на базе контейнеризации, развертывание внешних приманок, интеграция с внешними относительно композиции решения системами и инстанциями стека информационной безопасности. Принцип реализации решения сводятся к следующему: посредством

средств управления в инфраструктуре информационных технологий размещаются поддельные активы и ресурсы ложной среды, цель которых заключается в том, чтобы попасть под воздействие нарушителя. Развернутый комплекс инструментария подсистем был протестирован при помощи стороннего узла с соответствующим инструментарием и сценариями сканирования. Даны рекомендации по дальнейшему совершенствованию системы автоматизации развертывания и управления средств и мер технологии ложных компонент.

Информационный обман; технология ложных компонентов; ложные компоненты и системы; система автоматизации.

S.A. Smirnov, N.Yu. Parotkin, V.V. Zolotarev

AUTOMATION OF THE USE OF FALSE COMPONENTS IN THE INFORMATION SYSTEM

The article considers the applicability of deceptive information systems and their components in building an automated system for deploying and managing the applied implementation of deceptive component technology to improve the attack prevention system. The main advantages and the role of technology in the information security strategy setting the specifics and the area of technology means and tools practical appliance are suggested. The article considers the fundamentals of the architecture and features of the technology application, as well as its limitations. The purpose and the objective of using the present technology is pointed in terms of key principles of implementation disclosure. In addition, regulatory publications and other recommendations constituting the best practices in the field of its use were analyzed. The concept and architecture of the final automated solution for integration into information systems and security systems are considered, and the functional content of the final solution is described. A distinctive feature of the proposed solution is the use of controlled containerization mechanisms, that provide ample opportunities for scaling the solution and isolating compromised system components as a result of an intruder's actions. A formulated process of the automation system practical implementation in perspective of solution subsystems is schematically described in relation to dependent components (such as suggested document pieces and outer tools and systems) and included operations processing conditions. A model of deployment and operation of a distributed automation system is also provided in the following sequence: setting up a deployment server (including provisioning), deploying a network of false decoy components based on containerization, deploying external baits, integrating with systems and instances of the information security stack external to the composition of the solution. The solution is implemented by means of the principle: fake assets and resources of the fictive environment are deployed in an information technology infrastructure using controls and are intended to be affected by the adversary. The deployed set of subsystem tools was tested using a third-party node with the appropriate tools and scanning scenarios. Recommendations are given for further improvement of the automation system for deployment and management of tools and measures for deceptive component technology.

Cyber deception; deception technology; deceptive systems and components; automation system.

Введение. Исследования показывают [1–4], что со стороны злоумышленника особую обеспокоенность среди различных средств защиты вызывают системы обнаружения вторжений (СОВ) и технология ложных компонентов (ТЛК). В сочетании оба типа средств обеспечивают высокую вероятность обнаружение злоумышленника. Тем не менее, перед реализацией ТЛК на практике стоят некоторые концептуальные решения, требующие разрешения для целесообразного использования технологии в составе системы защиты. Так, необходима автоматизация в развертывании и настройке ложной сети (ЛС) компонентов, выступающих в качестве потенциальных целей для злоумышленника, которая дополнительно осложняется тем, что автоматизированному созданию подлежат уникальные сущности – ЛС, требующие комплексной настройки и технологического, информативного обеспечения. Таким образом, сама задача автоматизации создания ЛК выступает конструктивно сложной задачей, требующей многостороннего, интегративного в реализации технологии подхода. Данная необходимость вытекает не только из уникальных технологических мер и ограничений в обеспечении ложного информативного и прикладного пространства, но и – проработке ложного представления для ЛС как для потенциальной и целевой плоскости атаки и его исполнении на этапе планирования развертывания системы для ТЛК.

ТЛК является важнейшим элементом активной защиты и фокусируется на активном обнаружении несанкционированных действий внутри сети, оперативном устранении уязвимостей, сокрытии важной информации и отвлечении злоумышленников от производственных активов. Данная технология позволяет решить актуальные задачи, в том числе в составе СЗИ ГИС (меры ЗИС.27, ЗИС.28) [5]. В частности, можно выделить следующие преимущества ТЛК в составе СОВ [6–8]:

- существенное затруднение обхода злоумышленником действующей СЗ, препятствование доступа к подлинным активам посредством применения различных тактик и мер, позволяющих запутать атакующего;
- препятствование сбору подлинной и релевантной для злоумышленника информации об информационной системе (ИС) посредством внедрения ложного слоя потенциальных целей для атаки;
- минимизация ложных срабатываний, а, следовательно, и дополнительной нагрузки как на центры анализа данных, так и на системы обнаружения атак и мониторинга. Уведомления безопасности со стороны ТЛК считаются точными и к ним приставляется высокий уровень доверия, если технология развернута тактически верно;
- возможность сбора информации о тактиках. техниках, процедурах злоумышленника в ходе реализации им атаки – без рисков для защищаемых активов. На основе полученных сведений, СЗ может быть модифицирована соответствующими превентивными мерами защиты.

Автоматизированная ТЛК в составе СОВ позволяет обеспечить раннее обнаружение атак, дополняя систему возможностью обнаружения даже тех действий, что не были предотвращены действующей СЗ, что связано со спецификой концепции и принципами работы технологии.

1. Основы работы технологии ложных компонент. Как следует из названия технологии, ее основное назначение заключается в привлечении злоумышленника и его автоматизированных инструментов атаки таким образом, чтобы ими был осуществлен доступ к ложным информационным активам и ресурсам. Также ТЛК может быть развернута с целью сокрытия подлинных активов. Так, основное внимание при интеграции решения ТЛК фокусируется на управлении доступом и перенаправлении трафика, различных средствах маскирования подлинной информации [9, 12].

Аспект информационного обмана (ИО) в ТЛК строится на построении внешнего представления посредством манипулирования доступной информацией, сочетании подлинных и ложных данных [10, 11].

Реализация ТЛК предполагает взаимодополняющие основные аспекты, посредством которых и реализуется инфраструктура обмана:

- сокрытие подлинной ИС, ее ресурсов и активов;
- моделирование ложной ИС.

Принципы работы технологии сводятся к следующему: посредством централизованных средств управления в инфраструктуре информационных технологий (ИТИ) развертываются ловушки и размещаются приманки – поддельные активы и ресурсы построения ложной среды, цель которых заключается в том, чтобы попасть под воздействие нарушителя. Открытие файла приманки или использование поддельного пароля приводит к генерации уведомления безопасности и процессу идентификации злоумышленника. Ввиду изоляции ложных компонентов от производственных систем, попытки доступа к ловушкам указывают на факт вторжения злоумышленника и осуществления им несанкционированных действий, которые задействуют отправку оповещений безопасности и регистрацию действий в ЛК [13].

Тем не менее, средства ИО ТЛК могут быть размещены и в среде подлинной ИТИ [14, 15]. К подобным ЛК относятся *Honeytoken* и *Canarytoken*, способствующие обнаружению внутреннего нарушителя ИБ. Для того, чтобы приманки характеризовались правдоподобностью с точки зрения злоумышленника, могут использоваться навигационные компоненты – фрагменты информации, помещаемые в реальные активы, ведущие злоумышленника в реализуемой атаке непосредственно к ложным целям [16, 17].

Говоря об изоляции поддельного слоя информационной инфраструктуры от слоя подлинной инфраструктуры, следует отметить, что ложные объекты остаются неизвестны легитимным субъектам, что обеспечивается различными методами, например, сегментацией сети [18].

В настоящее время ТЛК представлена решениями – СЗИ класса *DDP (Distributed Deception Platform)* и *TDP (Threat Deception Platform)*, ориентированное в большей степени на активную ликвидацию угроз и уязвимостей) [19]. Подобные решения представляют собой системы управления распределенными ложными целями – сетевыми объектами, управляемыми централизованно при помощи сервера (и модуля управления) [20].

Модуль управления связывается с сервером развертывания ЛС таким образом, чтобы посредством получаемых команд осуществлять любые предусмотренные действия управления в отношении составляющих сеть ЛК. Непосредственные компоненты обеспечиваются средствами для регистрации действий, сбора и хранения получаемых данных, а также реагирования, либо включенных в состав соответствующих модулей на стороне сервера или центра управления – в зависимости от применяемой модели централизованного управления ЛК как целостной системой. ЛК – ловушки и эмулируемые сервисы соединены с сервером на постоянной основе, исключая при этом факт легитимного обращения к ним (т.е. вне предусмотренной в решении модели взаимодействия компонентов как правдоподобной сети) [20].

Современные решения технологии широко используют интеллектуальные подходы к формированию данных и приманок (в том числе, с применением ИИ), распознаванию атак, сбору и анализу ВПО, имитации правдоподобной активности в ложной инфраструктуре распределенных целей – и для многих других задач.

Отдельным вопросом при рассмотрении решений класса выступает возможность мониторинга состояния компонентов и ЛС в целом, который может быть разрешен как с использованием агентурной системы, так и без нее; при этом каждый метод связан с соответствующими издержками в реализации итоговой модели функционирования решения.

2. Система автоматизации создания ложных целей в рамках технологии ложных компонентов. Одной из актуальных задач, стоящих перед ТЛК, выступает автоматизация создания и настройки разнотипных ЛК, поскольку ручное оперирование процессами связано с существенными издержками; проблематика обусловлена сущностью технологии, предполагающей эмуляцию достоверной, многообразной по своему содержанию ИТИ, в своей вариативности обладающему чертами индивидуальности, аутентичности для каждой отдельной ИС.

Определим методы автоматизации процессов развертывания ЛС. В качестве отдельных групп управляемых процессов в существе развертывания инфраструктуры ЛК можно выделить следующие:

- создание типовых контейнерных ЛК в масштабируемом количестве и централизованная настройка ложной сети;
- генерация, распространение, размещение в ЛС компонентов-приманок (файлов) – ложных данных;
- конфигурирование контейнерных ЛК-ловушек как отдельных уникальных, либо типовых единиц;
- развертывание и настройка служб, сервисов и протоколов ИТИ для формирования уникального содержания представления высокоуровневых ЛК;
- настройка и обеспечение функционирования входящих в состав решения средств, инструментов, тиражируемых по ложным средам для регистрации действий злоумышленника и в других целях, стоящих перед решением.

Управление созданием распределенной ЛС целей можно, таким образом, разделить на логические этапы:

1) начальный: развертывание и настройка средств сервера централизованного управления компонентами решения, а также обеспечение связей интеграции с другими СЗИ и модулями управления. Также на данном этапе определяются параметры сети ложной инфраструктуры, ее топология;

2) настройка и создание эталонных компонентов, используемых как типовой основы для дальнейшей реализации ИО, обладающих некоторой базовой конфигурацией и необходимым набором средств решения вне ИО;

3) автоматизированная генерация и распространение независимых уникальных экземпляров приманок для наполнения интерактивных ЛК сети. Поскольку соответствие отдельного экземпляра ложных данных и конкретной системы (ловушки) не требуется, данный процесс может протекать изолированно от прочих целенаправленных операций с ловушками;

4) конфигурирование отдельных ЛК и развертывание служб, сервисов и приложений в целях ИО.

Рассмотрим модули решения. Были выделены следующие сущности:

♦ сервер развертывания: виртуальная или реальная система, обеспечивающая технологические действия с распределенными ложными целями;

♦ центр управления: функционал управления может быть локализован как на непосредственном сервере, так и вынесен на удаленные системы;

♦ модуль анализа: вынесен на внешнюю систему *SIEM*;

♦ модуль обнаружения вторжений и регистрации: исполняется разнородными средствами, обеспечивающими создание ЛК;

♦ модуль передачи данных: настроенное взаимодействие сервера и клиента для передачи журналов событий.

Далее представлена модель (схема) функционирования решения в рамках системы автоматизации создания ложных целей посредством ЛС решения (рис. 1). Цветом выделены процессы, внешние относительно исполняемой в исследовании системы решения и рекомендованные для использования в составе обеспечивающего его комплекса. Модель иллюстрирует реализованные аспекты автоматизации в управлении решением и затрагивают не только процесс создания ЛС, но и – внесение, удаление отдельных ЛК, уничтожение ЛС; данная совокупность автоматизируемых операций названа масштабированием. В основе модели лежит разделение на описанные подсистемы решения.

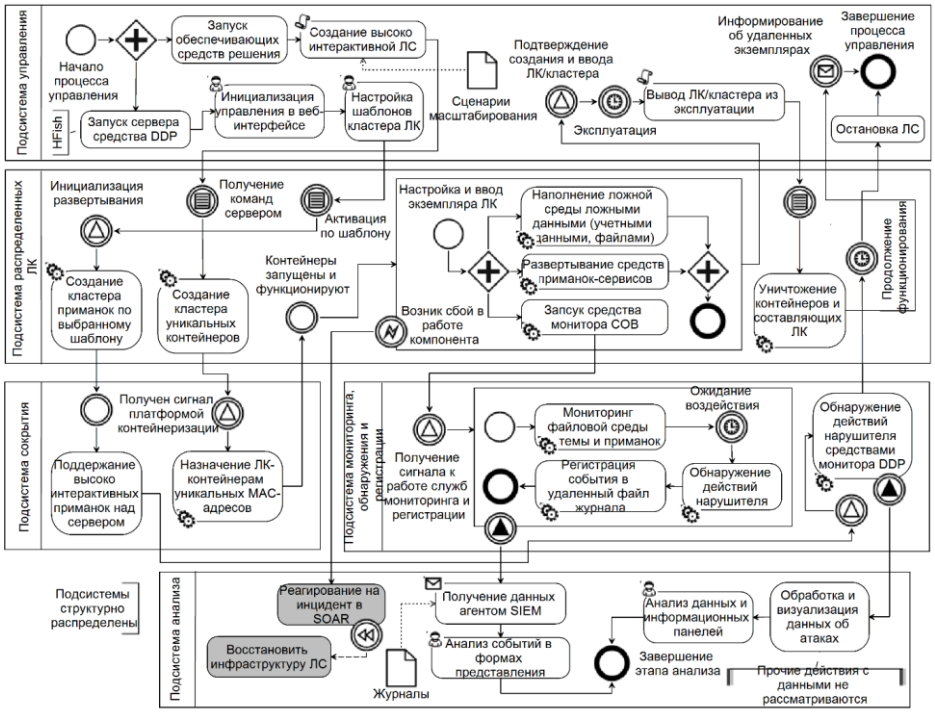

Рис. 1. Схема исполнения решения в системе автоматизации (BPMN 2.0)

При этом, для определяемой системы характерна модель информационных потоков (рис. 2). Данная модель иллюстрирует роли интеграций компонентов, реализующих ИО, с внешними обеспечивающими системами и демонстрирует общую сложность системы автоматизации. Произведено разделение на внешние сущности, процессы (операции) и инстанции хранения данных – связанные каналами передачи данных и управления.

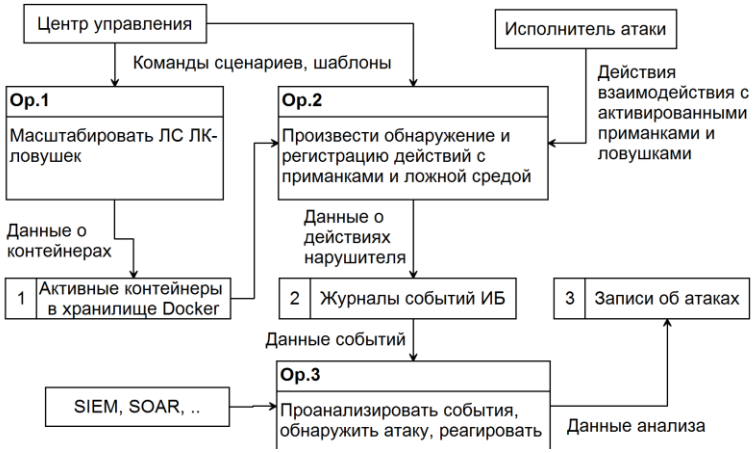

Рис. 2. Схема информационных потоков в рамках системы решения (DFD)

Как видно по схемам выше, потоки сосредоточены на нескольких категориях (передачи) данных: инициирующие активности и операции воздействия, данные событий действий нарушителя и данные для мониторинга.

Схема развертывания системы решения, включая необходимые предполагаемые интеграции с соответствующими средствами и системами (защиты), представлена на рис. 3.

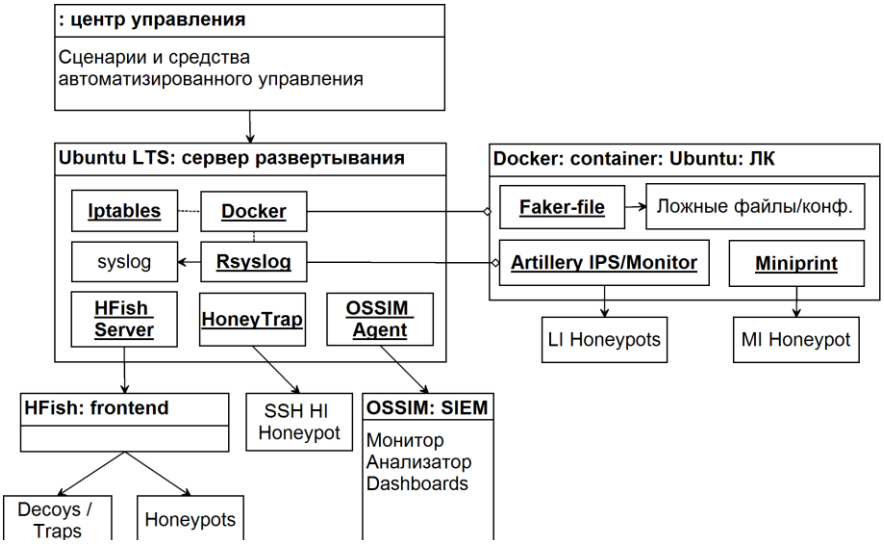

Рис. 3. Схема развертывания системы решения (UML Deployment)

Первым шагом были протестированы возможности *Honey Trap*. Было произведено подключение к узлу по *ssh*. При этом осуществлялось перенаправление в ложную среду. Следующим шагом производилось сканирование эмулируемого устройства *Miniprint*. При попытке сканирования сервер также отзывался соответствующими уведомлениями. Далее производилось сканирование приманок, развернутых средствами *Artillery*. До запуска сервера сетевое представление ЛК-контейнера содержит только фильтруемый порт

передачи *Syslog*. После запуска сервера произведем простое сканирование *Nmap* портов и сетевых служб, а также сканирование уязвимостей, результатом которого стало обнаружение 15 новых служб.

Далее произведем сканирование приманок платформы *HFish* и сопоставим результаты. На рис. 4 продемонстрировано сканирование адреса сервера развертывания, на котором функционируют приманки платформы, средствами *Nmap* с использованием сценария выявления уязвимостей *Vulscan*.

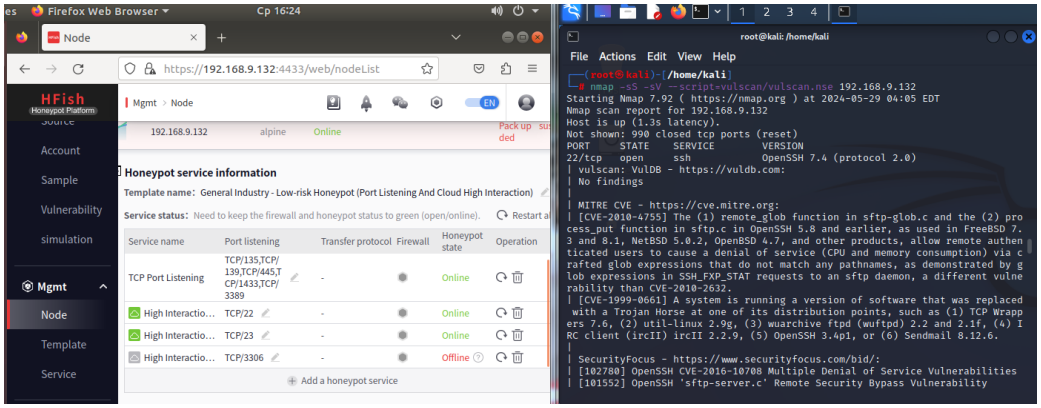

Рис. 4. Сканирование HFish с использованием сценария .NSE (Nmap)

Таким образом было произведено взаимодействие различных уровней интерактивности внешней стороны (нарушителя) с сетевым представлением, сформированным комплексом ложных компонентов. В результате отмечена работоспособность всех развернутых компонентов, паттерны применения мер ИО со стороны не выявлены.

Описанными средствами также достигается некоторое сокрытие сервера: *ssh*-трафик перенаправляется в ложную среду, тогда как результаты сканирования предоставляют информацию злоумышленнику, формируя недостоверную картину сетевого представления узла – тогда как сам сервер защищен межсетевым экраном и СОВ.

Заключение. По результатам исследования была разработана комплексная система автоматизации создания ложных целей в рамках уникального многокомпонентного решения технологии в составе системы предупреждения вторжений. Так, было произведено решение основных стоявших в рамках исследования проблем использования технологии, сформулирована и протестирована возможность построения системы автоматизации, распределенной в решении, построенного в соответствии с принципами *DevOps* и модульным подходом. Система решения не представляет собой итоговую и полностью обеспеченную модель для отдельных специфических информационных систем, но демонстрирует логику и возможность использования автоматизированных и осуществимых подходов в масштабировании средств технологии ложных компонентов, их интеграции в систему защиты и практического использовании мер информационного обмана.

Тем не менее, в дальнейшем, в зависимости от реализуемого функционала, рекомендуется интеграция комплекса решения с *SOAR*. Помимо этого, на основании результатов исследования данной главы рекомендуется построение системы эмуляции ложной активности – и прочие продвинутые техники и методы информационного обмана ТЛК, обеспечивающие привлекательность ложных целей. Подобные аспекты не были затронуты в рамках исследования, поскольку выходят за границы изначальной цели в образовании системы автоматизации непосредственного создания ложных целей – а не обеспечения их уникальной сущности функционирования в перспективе. Так, работа затрагивает именно первоначальный этап автоматизированного развертывания средств и мер ТЛК и построения необходимых для дальнейших процессов управления связей.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Crandall C., Salazar J.* Deception-Based Threat Deception: Shifting power to the defenders. – Attivo Networks, inc: 2019. – vi, 116 p. – URL: https://www.bankinfosecurity.com/whitepapers/deception-based-threat-detection-shifting-power-to-defenders-w-5780 (дата обращения: 07.01.2024).
2. ITRC: 2023 Data Breach Report / Identity Theft Resource Center: 2024. – 40 p. – URL: https://www.idtheftcenter.org/ publication/2023-data-breach-report/ (дата обращения: 13.03.2024).
3. SCALE: Cybersecurity Perspectives 2023 / SCALE. – 20 p. – URL: https://www.scalevp.com/wp-content/uploads/2023/10/Scale-Security-Report-2023-Final.pdf (дата обращения: 14.03.2024).
4. Attivo Networks: Defending Against Insider Threats with Attivo Networks: whitepaper / Attivo Networks, 2019. – 5 p. – URL: https://www.bankinfosecurity.com/whitepapers/defending-against-insider-threats-attivo-networks-w-5784 (дата обращения: 14.03.2024).
5. Методический документ. Меры защиты информации в государственных информационных системах: методический документ ФСТЭК: издание официальное: утвержден 11 февраля 2014 г.: введен впервые: дата введения 2014-02-11. – М.: ЗАО «Кодекс», 2014. – 128 с.
6. *Bellekens X.* How Does Cyber Deception Work and Why Should you Care? – URL: https://www.lupovis.io/how-does-cyber-deception-work/ (дата обращения: 07.01.2024).
7. *Strand J., Asadoorian P. [и др.].* Offensive Counter-measures: The Art of Active Defense. – Self-published. – 2017. – 167 p. – ISBN: 1974671690.
8. *Lachow I.* Active Cyber Defense: A framework for Policymakers. – Vol. 2022. – Article ID 3949292. – 17 p. – URL: https://www.cnas.org/publications/reports/active-cyber-defense-a-framework-for-policymakers (дата обращения: 15.03.2024).
9. *Srinivasa S., Pedersen M. [и др.].* Gotta catch' em all: A Multistage Framework for Honeypot fingerprinting. – 26 p. – URL: https://www.researchgate.net/publication/354776911 (дата обращения: 15.03.2024).
10. *Cohen E.* DECEPTION: TYPES, PRINCIPLES, AND TACTICS // IS: The International Journal of an Emerging Transdiscipline. – 2019. – Vol. 22. – P. 137-156. – DOI: 10.28945/4487. – URL: https://www.researchgate.net/publication/344634437 (дата обращения: 19.01.2024).
11. *Wang C., Lu Z.* IEEE Security Cyber Deception Overview and The Road Ahead // IEEE Security and Privacy Magazine. – IEEE, 2018. – 16 (2). – P. 80-85. – DOI: 10.1109/MSP.2018.1870866. – URL: https://www.researchgate.net/publication/324117795 (дата обращения: 17.01.2024).
12. *Путято М.М., Макарян А.С. [и др.].* Исследование применения технологии deception для предотвращения угроз кибербезопасности // Прикаспийский журнал: управление и высокие технологии. – 2020. – № 4 (52). – DOI: 10.21672/2074-1707.2020.52.4.085-098. – 14 p. – URL: https://hi-tech.asu.edu.ru/?articleId=1260 (дата обращения: 16.03.2024).
13. Advanced Threat Protection: Threat Detection and Threat Prevention: Tools and Tech. – URL: https://www.cynet.com/advanced-threat-protection/threat-detection-and-threat-prevention-tools-and-tech/ (дата обращения: 29.03.2022).
14. *Li Zhang., Thing L*. Three Decades of Deception Techniques in Active Cyber Defense – Retrospect and Outlook. – 19 p. – URL: https://www.researchgate.net/publication/350750138 (дата обращения: 16.04.2024).
15. *Islam M.M., Al-Shaer E.* Active Deception Framework: An Extensible Development Environment for Adaptive Cyber Deception // 2020 IEEE Secure Development (SecDev). – Conference: IEEE 28-30 September 2020. – P. 41-48. – DOI: 10.1109/SecDev45635.2020.00023. – URL: https://ieeexplore.ieee.org/document/9230100 (дата обращения: 26.04.2024).
16. *Heckman K.E., Stech F.J. [и др.].* Denial and Deception in Cyber Defense. The MITRE Corporation // IEEE. – Computer. – 2015. – Vol. 48, Issue 4. – P. 36-44. – DOI: 10.1109/MC.2015.104. – URL: https://ieeexplore.ieee.org/abstract/document/7085646 (дата обращения: 30.04.2024).
17. *Mizrahi R.* Deploying Deception in the Enterprise Network. – URL: https://www.darkreading.com/attacks-breaches/deploying-deception-in-the-enterprise-network (дата обращения: 30.03.2022).
18. *Bowcut S.* Decoys, Deception Sensors, and Breadcrumb Data – What's a Hacker To Do? – URL: https://brilliancesecuritymagazine.com/cybersecurity/decoys-deception-sensors-and-breadcrumb-data-whats-a-hacker-to-do/ (дата обращения: 11.04.2022).
19. R-Vision Threat Deception Platform. – Имитация ИТ-инфраструктуры для обнаружения кибератак / R-Vision. – 4 p. – URL: https://rvision.ru/storage/2022/04/07/hN63FoYRijfyBKiYGx3Dytc1QhrZklagh0K9WYbr.pdf (дата обращения: 10.04.2022).
20. *Бортников С.* Использование ловушек (Deception) для обнаружения злоумышленников в инфраструктуре. – URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Intruder-Detection-Using-Deception (дата обращения: 09.05.2024).

REFERENCES

1. *Crandall C., Salazar J.* Deception-Based Threat Deception: Shifting power to the defenders. Attivo Networks, inc: 2019, vi, 116 p. Available at: https://www.bankinfosecurity.com/whitepapers/deception-based-threat-detection-shifting-power-to-defenders-w-5780 (accessed 07 January 2024).
2. ITRC: 2023 Data Breach Reportб Identity Theft Resource Center: 2024б 40 p. Available at: https://www.idtheftcenter.org/ publication/2023-data-breach-report/ (accessed 13 March 2024).
3. SCALE: Cybersecurity Perspectives 2023, SCALE, 20 p. Available at: https://www.scalevp.com/wp-content/uploads/2023/10/Scale-Security-Report-2023-Final.pdf (accessed 14 March 2024).
4. Attivo Networks: Defending Against Insider Threats with Attivo Networks: whitepaper, Attivo Networks, 2019, 5 p. Available at: https://www.bankinfosecurity.com/whitepapers/defending-against-insider-threats-attivo-networks-w-5784 (accessed 14 March 2024).
5. Metodicheskiy dokument. Mery zashchity informatsii v gosudarstvennykh informatsionnykh sistemakh: metodicheskiy dokument FSTEK [Methodological document. Information security measures in state information systems: FSTEC methodological document]: official publication: approved on February 11, 2014: introduced for the first time: date of introduction 2014-02-11. Moscow: ZAO «Kodeks», 2014, 128 p.
6. *Bellekens X.* How Does Cyber Deception Work and Why Should you Care? Available at: https://www.lupovis.io/how-does-cyber-deception-work/ (accessed 07 January 2024).
7. *Strand J., Asadoorian P. [u ðp.].* Offensive Counter-measures: The Art of Active Defense. Self-published, 2017, 167 p. ISBN: 1974671690.
8. *Lachow I.* Active Cyber Defense: A framework for Policymakers, Vol. 2022, Article ID 3949292, 17 p. Available at: https://www.cnas.org/publications/reports/active-cyber-defense-a-framework-for-policymakers (accessed 15 March 2024).
9. *Srinivasa S., Pedersen M. [u ðp.].* Gotta catch' em all: A Multistage Framework for Honeypot fingerprinting, 26 p. Available at: https://www.researchgate.net/publication/354776911 (accessed 15 March 2024).
10. *Cohen E.* DECEPTION: TYPES, PRINCIPLES, AND TACTICS, *IS: The International Journal of an Emerging Transdiscipline,* 2019, Vol. 22, pp. 137-156. DOI: 10.28945/4487. Available at: https://www.researchgate.net/publication/344634437 (accessed 19 January 2024).
11. *Wang C., Lu Z.* IEEE Security Cyber Deception Overview and The Road Ahead, I*EEE Security and Privacy Magazine*. IEEE, 2018, 16 (2), pp. 80-85. DOI: 10.1109/MSP.2018.1870866. Available at: https://www.researchgate.net/publication/324117795 (accessed 17 January 2024).
12. *Putyato M.M., Makaryan A.S. [i dr.].* Issledovanie primeneniya tekhnologii deception dlya predotvrashcheniya ugroz kiberbezopasnosti [Study of the application of deception technology to prevent cybersecurity threats], *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Management and High Technologies], 2020, No. 4 (52). DOI: 10.21672/2074-1707.2020.52.4.085-098, 14 p. Available at: https://hi-tech.asu.edu.ru/?articleId=1260 (accessed 16 March 2024).
13. Advanced Threat Protection: Threat Detection and Threat Prevention: Tools and Tech. Available at: https://www.cynet.com/advanced-threat-protection/threat-detection-and-threat-prevention-tools-and-tech/ (accessed 29 March 2024).
14. *Li Zhang., Thing L*. Three Decades of Deception Techniques in Active Cyber Defense – Retrospect and Outlookб 19 p. Available at: https://www.researchgate.net/publication/350750138 (accessed 16 April 2024).
15. *Islam M.M., Al-Shaer E.* Active Deception Framework: An Extensible Development Environment for Adaptive Cyber Deception, *2020 IEEE Secure Development (SecDev). Conference: IEEE 28-30 September 2020,* pp. 41-48. DOI: 10.1109/SecDev45635.2020.00023. Available at: https://ieeexplore.ieee.org/document/9230100 (accessed 26 April 2024).
16. *Heckman K.E., Stech F.J. [u ðp.].* Denial and Deception in Cyber Defense. The MITRE Corporation, *IEEE. Computer,* 2015, Vol. 48, Issue 4, pp. 36-44. DOI: 10.1109/MC.2015.104. Available at: https://ieeexplore.ieee.org/abstract/document/7085646 (accessed 30 April 2024).
17. *Mizrahi R.* Deploying Deception in the Enterprise Network. Available at: https://www.darkreading.com/attacks-breaches/deploying-deception-in-the-enterprise-network (accessed 30 March 2022).
18. *Bowcut S.* Decoys, Deception Sensors, and Breadcrumb Data – What's a Hacker To Do? Available at: https://brilliancesecuritymagazine.com/cybersecurity/decoys-deception-sensors-and-breadcrumb-data-whats-a-hacker-to-do/ (accessed 11 April 2022).
19. R-Vision Threat Deception Platform. – Имитация ИТ-инфраструктуры для обнаружения кибератак / R-Vision. – 4 p. Available at: https://rvision.ru/storage/2022/04/07/hN63FoYRijfyBKiYGx3Dytc1QhrZklagh0K9WYbr.pdf (accessed 10 April 2022).
20. *Bortnikov S.* Ispol'zovanie lovushek (Deception) dlya obnaruzheniya zloumyshlennikov v infrastructure [Using traps (Deception) to detect intruders in the infrastructure]. Available at: https://www.anti-malware.ru/analytics/Technology_Analysis/Intruder-Detection-Using-Deception (accessed 09 May 2024).

Смирнов Семен Александрович – Сибирский университет науки и технологий; e-mail: simon.simriel@gmail.com; г. Красноярск, Россия; тел.: 89130407272; кафедра безопасности информационных технологий; аспирант.

Паротькин Николай Юрьевич – e-mail: nyparotkin@yandex.ru; тел.: 89509920640; кафедра безопасности информационных технологий; к.т.н.; доцент.

Золотарев Вячеслав Владимирович – e-mail: zolotorev@sibsau.ru; тел.: 89059738091; кафедра безопасности информационных технологий; зав. кафедрой; к.т.н.

Smirnov Simon Aleksandrovich – Siberian University of Science and Technology; e-mail: simon.simriel@gmail.com; Krasnoyarsk, Russia; phone: +79130407272; the Department of Information Technology Security; post graduate student.

Parotkin Nikolay Yuryevich – e-mail: nyparotkin@yandex.ru; phone: +79509920640; the Department of Information Technology Security; cand. of eng. sc.; associate professor.

Zolotarev Vyacheslav Vladimirovich – e-mail: zolotorev@sibsau.ru; phone: +79059738091; the Department of Information Technology Security; head of department; cand. of eng. sc.

УДК 004.056 DOI 10.18522/2311-3103-2024-6-218-229

В.Г. Жуков, С.В. Селигеев

ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ ИМЕНОВАНИЯ И ИДЕНТИФИКАЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ПРОЦЕССАХ УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ

Управление ИТ активами является базисом для построения эффективного процесса управления уязвимостями. Не имея представления о контролируемых ИТ активах, технически невозможно начать построение процесса управления уязвимостями. При наличии действующего процесса управления ИТ активами, одной из задач, являющейся важной для управления уязвимостями, является однозначное именование программного обеспечения как актива. Такое однозначное именование позволяет идентифицировать программное обеспечение и его уязвимости без применения активного сканирования узлов ИТ инфраструктуры, а только при помощи взаимодействия с системой управления ИТ активами. Технически данный подход можно назвать «пассивное обнаружение уязвимостей», однако использование существующих систем именования для его реализации является крайне трудоемкой задачей. Для того чтобы сделать пассивное обнаружение реальным, в работе авторами предлагается создать общий фундамент путем формирования концептуальной схемы и последующего создания системы стандартизированного именования и идентификации программного обеспечения, регулирование которой будет происходить централизованно на государственном уровне. В рамках рассмотрения существующих систем именования программного обеспечения, внимание уделяется проблемам CPE как со стороны специалистов на местах, а именно получение CPE-идентификаторов и трансляция информации о программном обеспечении в CPE-идентификатор, так и со стороны агрегатора данных об уязвимостях, а именно получение сведений об уязвимостях через CPE-идентификатор. Обнаруженные в ходе исследования проблемы применения CPE, а также проблемы взаимодействия с агрегаторами данных об уязвимостях из недружественных стран формируют предпосылки к формированию национальной системы государственного регулирования именования и идентификации программного обеспечения, которая устранит проблемы существующих систем именования программного обеспечения. В заключении приводятся преимущества национальной системы именования и идентификации программного обеспечения в случае ее создания и использования в реальных условиях всеми участниками процесса управления уязвимостями.

Информационная безопасность; управление уязвимостями; управление активами; CPE.