МАСКИРОВАНИЕ СТРУКТУРЫ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ В КИБЕРПРОСТРАНСТВЕ

Ворончихин И.С.[1], Иванов И.И.[2], Максимов Р.В.[3], Соколовский С.П.[4]

Формулируя требования по защите информации, регуляторы предписывают необходимость учитывать при определении угроз безопасности структурно-функциональные характеристики информационной системы, включающие структуру и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи между сегментами информационной системы, применяемые информационные технологии и особенности их функционирования. В качестве основных мер по защите предлагают эмуляцию ложных компонентов информационных систем, скрытие истинных информационных технологий, управление конфигурацией информационной системы и перевод ее в заранее определенную конфигурацию, обеспечивающую защиту. Однако по ряду причин такие меры не включают в базовый набор и реализуют достижение целей защиты компенсирующими средствами, формализуя и внедряя запрещающие регламенты, а также набор организационных и технических мер воздействия на источник опасности.

Цель исследования – вскрыть и сформулировать основные направления поиска новых технических решений для маскирования структуры распределенных информационных систем в киберпространстве, устраняя антагонизм атакующей и защищающейся сторон.

Метод исследования – обфускация состава, структуры и алгоритмов функционирования распределенных информационных систем в киберпространстве. Описание сформулированных принципов и разработанных технологий маскирования приводится в терминологии концепции Moving Target Defense.

Результат исследования – ассортимент технических решений по маскированию информационных систем, интегрированных с сетью связи общего пользования. Полученные результаты позволяют явно реализовывать меры защиты, направленные на формирование у нарушителей устойчивых ложных стереотипов об информационных системах и процессах управления, реализуемых с их помощью.

Ключевые слова: *moving target defense, компьютерная разведка, информационные направления, проактивная защита, сетевое адресное пространство, навязывание ложной структуры.*

DOI: 10.21681/2311-3456-2019-6-92-101

Введение

Расширение областей применения информационных технологий под воздействием растущих информационных потребностей должностных лиц порождает новые угрозы информационной безопасности и, как следствие, рост масштабов компьютерной преступности. Наиболее актуальными в настоящее время предпосылками к возникновению угроз информационной безопасности являются:

- недекларированные возможности аппаратного и программного обеспечения (ПО), обусловленные использованием зарубежной технологической базы;
- вынужденная необходимость использовать услуги операторов связи (провайдеров), которые определяют принципы маршрутизации и коммутации трафика для предоставления сервиса виртуальной частной сети (*Virtual Private Network, VPN*), и могут пользоваться услугами сторонних провайдеров (в том числе и зарубежных);
- расширение ассортимента технических средств компьютерной разведки (КР), доступных злоумышленникам;
- снижение «порога вхождения» в деятельность, связанную с компьютерной преступностью, что привело к возникновению понятия «вымогатель как услуга» (*Ransomware as a Service, RaaS*), при которой разработчики вредоносного ПО не являются организаторами компьютерных атак (КА), а зарабатывают на его продаже преступным группировкам;
- увеличение количества ботнетов (от англ. *robot network* – сеть, состоящая из зараженных вре-

1 Ворончихин Иван Сергеевич, адъюнкт, Краснодарское высшее военное училище, г. Краснодар, Россия. E-mail: 5.00@mail.ru

2 Иванов Илья Игоревич, научный сотрудник, Краснодарское высшее военное училище, г. Краснодар, Россия. E-mail: 7570745@mail.ru

3 Максимов Роман Викторович, Заслуженный изобретатель Российской Федерации, доктор технических наук, профессор, профессор кафедры, Краснодарское высшее военное училище, г. Краснодар, Россия. E-mail: rvmaxim@yandex.ru

4 Соколовский Сергей Петрович, кандидат технических наук, доцент, докторант, Краснодарское высшее военное училище, г. Краснодар, Россия. E-mail: ssp.vrn@mail.ru

доносным ПО компьютеров), предназначенных для реализации КА типа «отказ в обслуживании» (*Denial of Service, DoS*), и их производительности за счет развития концепции «Интернет вещей» (*Internet of Things, IoT*);
- увеличение ассортимента уязвимостей в коммуникационном оборудовании[5].

В ведомственных информационных системах (ИС) кибербезопасность и защита киберпространства реализуется как набор мер и рекомендаций регуляторов[6]. Однако на текущий момент отсутствуют технические решения, которые позволяют реализовать меры безопасности, направленные на обеспечение:
- имитации функционирования реальной ИС для обнаружения и предотвращения КР и КА;
- навязывания злоумышленнику ложной информации и снижение возможности успешной реализации КА;
- управления изменением конфигурации ИС или ее сегментов и системы защиты;
- защиты информации от раскрытия, модификации и навязывания при ее передаче по каналам связи, имеющим выход за пределы контролируемой зоны;
- обнаружения, идентификации, а также принятие мер по устранению и предупреждению инцидентов.

Рассмотрим теоретические предпосылки и ассортимент технических возможностей для реализации перечисленных мер для маскирования структуры распределенных ИС в киберпространстве.

1. Функционирование распределенных информационных систем в киберпространстве

Под термином «кибербпространство» в данной работе будем понимать определение, редуцированное из приведенного в [1]. Киберпространство – это виртуальная сетевая среда, сформированная в результате действий пользователей, программ и сервисов в сети связи общего пользования посредством коммуникационных технологий.

В соответствии с данным определением ИС, функционирующие в киберпространстве, представляют собой совокупность территориально распределенных сегментов, объединенных каналами связи различной протяженности с использованием коммуникационных технологий (оборудования) через сети связи общего пользования (ССОП) с целью предоставления пользователям ИС информационных ресурсов (программ и сервисов).

Доступ к разделяемым (между пользователями) информационным ресурсам распределенных ИС осуществляют с использованием протоколов сетевого взаимодействия, которые реализованы в коммуникационном оборудовании (коммутаторы, маршрутизаторы) и оконечных устройствах (локальных и удаленных).

Наличие в таких распределенных ИС инфраструктурных элементов, не контролируемых системой защиты (линии связи большой протяженности, коммуникационное оборудование провайдеров), создает условия для перехвата пакетов сообщений, передаваемых по каналам связи, реконструкции функционально-логической структуры распределенной ИС, и реализации КА. Функционально-логическая структура формируется (реконструируется) КР злоумышленника на основе логического анализа перехваченных пакетов сообщений и отражает коммуникационные узлы, идентифицированные сетевыми адресами, и логические связи между ними по признаку наличия взаимного информационного обмена с указанием его интенсивности и направления.

Таким образом, распределенным ИС присущи следующие особенности, расширяющие возможности КР и повышающие ее результативность [2]:
- топологическое распределение элементов инфраструктуры;
- наличие элементов инфраструктуры, не охваченных системой защиты;
- совместное использование элементов ССОП разными провайдерами;
- значительный ассортимент альтернатив маршрутизации трафика;
- разнородность используемого коммуникационного оборудования и каналов связи;
- непрерывное усложнение ИС под влиянием растущих информационных потребностей должностных лиц;
- открытость архитектуры ИС, которая способна обеспечить удовлетворение растущих информационных потребностей должностных лиц.

Функционально-логическая структура тривиально реконструируется по идентификаторам коммуникационных узлов, представляющим собой именные демаскирующие признаки (ДМП) корреспондентов, и интенсивности трафика, связанной с уровнем иерархии узла.

Перед осуществлением КА злоумышленник проводит КР, в ходе которой добывает данные о структуре ИС, используемых устройствах, ПО и его версиях, возможных уязвимостях и применяемых средствах защиты, а использование схожих архитектурных решений ИС облегчает процесс проведения КР [3].

2. Средства компьютерной разведки

Современные средства КР позволяют в режиме реального времени выполнять отбор трафика по заданным признакам (адреса отправителя и получателя, используемые протоколы и порты). Поэтому даже при отсутствии возможности декодирования перехваченной информации основная часть логики функционирования распределенной ИС доступна злоумышленнику через ДМП информационного обмена [4, 5]. Конструктивное использование злоумышленником такой информации заключается в попытках осуществлять НСД, подавлять критически важные узлы распределенной ИС, модифицировать трафик, снижать качество обслуживания тра-

5 Актуальные киберугрозы. Тренды и прогнозы. URL: https://axoft.ru/upload/iblock/3cb/Cybersecurity-threatscape-2017-rus.pdf

6 Например, см. Приказы ФСТЭК России №№ 17, 21, 31, 239, ГОСТ Р ИСО 27001 и др.

фика и узлов связи, входящих в маршрут информационного обмена.

Для того чтобы корректно перейти к описанию возможностей КР, необходимо дать ей конструктивное определение. Известны [4, 6] два основных варианта такого определения. Представленное в [6] не включает конкретной информации об объекте разведки и его элементах, поэтому наиболее конструктивным представляется подход авторов в [4].

Компьютерная разведка – процесс, направленный на добывание информации о составе, структуре и алгоритмах функционирования, местоположении и принадлежности ИС, данных, хранимых, обрабатываемых и передаваемых в ИС и осуществляемый путем организации и реализации диалогового (процедурного) взаимодействия с элементами ИС, которым присущи недекларированные возможности, уязвимости и открытость архитектуры.

В соответствии с таким определением схема распределенной ИС может и должна быть представлена в виде объединения распределенных сегментов (подсетей) посредством ССОП, находящейся под административным контролем провайдеров, и технических средств КР злоумышленника. Расположение технических средств КР злоумышленника между защищаемыми сегментами заранее неизвестно, однако очевидно, что злоумышленник решает ресурсную задачу по распределению неоднородных ограниченных средств КР так, чтобы осуществлять оптимальный мониторинг распределенной структуры (с точки зрения полноты охвата, своевременности и достоверности получаемой им информации). Технологически такая задача может решаться созданием виртуальных точек присутствия, методически – решением задачи о минимальном разрезе графа.

В процессе вскрытия функционально-логической структуры злоумышленнику необходимо идентифицировать в перехваченных пакетах сообщений параметры, которые остаются неизменными в течение времени – инварианты ИС [4]. В работе [5] представлена классификация инвариантов, необходимых для синтеза адекватных моделей: инварианты состава, структуры и алгоритмов функционирования ИС. Выявление инвариантов ИС происходит путем получения (перехвата) и анализа ДМП.

Даже при условии реализации мер защиты злоумышленник имеет широкие возможности по анализу инвариантов ИС, так как факт передачи информации по скомпрометированному каналу скрыть невозможно даже при использовании *VPN*. Причем если передаваемую информацию защищают криптографическими методами, то данные о составе, структуре и алгоритмах функционирования ИС всегда доступны для анализа в перехваченных пакетах сообщений и востребованы злоумышленником. В результате злоумышленник имеет преимущество перед системой защиты, которое выражается в практически неограниченном времени на КР и подготовку КА, тогда как для реализации КА достаточно успешной эксплуатации одной уязвимости.

3. Принципы противодействия конфликтующих сторон

Для описания принципов противодействия конфликтующих сторон применяются [4] так называемые базовые защитные установки: дистанцирование со злоумышленником; управление каналами воздействия; управление информационными потоками.

Использование первой установки реализует принцип пространственного обеспечения безопасности путем увеличения дистанции между ИС и злоумышленником. Архаичные ИС обособлялись как территориально (топологически), так и снижением электромагнитной доступности защищаемой системы. Эволюция инфраструктур привела к их глобализации и трансграничности, поэтому построение выделенных ИС не соответствует современным требованиям должностных лиц и стремлению к формированию единого информационного пространства.

Использование второй установки заключается в обеспечении безопасности путем формализации и внедрения ассортимента запрещающих регламентов, а также набора организационных и технических мер воздействия на источник опасности. Система обеспечения информационной безопасности в данном случае не может в полной мере и всесторонне охватить своими регламентами информационную инфраструктуру и технологии, а на неподконтрольные ей элементы вводит совокупность ограничений и запретов. Другими словами, системе обеспечения информационной безопасности приходится подавлять разнообразие состояний распределенной ИС, чтобы сохранить устойчивость управления. Неизбежный результат – снижение эффективности инновационной деятельности в сфере информационных технологий, поражение в конкуренции с системами, поощряющими рост разнообразия.

Использование третьей установки заключается в том, что устраняется антагонизм атакующей и защищающейся сторон. Это достигается тем, что применение установки дает возможность сделать цели сторон или независимыми, или совпадающими. Если принять, что злоумышленник предъявляет к ИС требование информативности, а система защиты является источником информационных сообщений для системы злоумышленника, то необходимо формировать неверные эталоны с использованием всего многообразия возможных состояний ИС (маскировать её). Реализовать такой принцип защиты возможно тогда, когда разнообразие состояний, допускаемых регламентом обеспечения информационной безопасности, будет не меньше, чем потенциальное разнообразие состояний ИС.

В процессе эволюции информационных технологий и инфраструктур информационное противоборство сместилось в третью защитную установку, тогда как системы обеспечения информационной безопасности в основном остановились на второй. Поэтому традиционные средства и методы борьбы с угрозами сетевой безопасности основаны на использовании межсетевых экранов, сетевых фильтров, систем обнаружения вторжений, сканеров безопасности, иными словами на обнаружении факта совершения КР или КА и реагирова-

нии на него и не способны эффективно противостоять современным техническим средствам КР [7].

4. Концепция *Moving Target Defense*

Одним из подходов, реализующих третью установку и, как следствие, проактивную систему защиты, является концепция, которая получила название *Moving Target Defense* (*MTD*). Суть концепции заключается в замене статических параметров ИС динамическими, в результате чего злоумышленник не может получить актуальную информацию, позволяющую реализовать уязвимости.

В концепции *MTD* принято выделять [8] следующие пять основных направлений (рис.1).

Динамическое изменение ПО (*dynamic software*), которое заключается в обфускации программного кода приложения: применение компиляторов, рандомизирующих машинный код, вставка мертвого кода, перестановка местами инструкций, базовых блоков и функций, замена инструкций на эквивалентные, шифрование буферов данных.

Динамическое изменение данных (*dynamic data*), заключающееся в изменении формата, синтаксиса и представления данных приложения, чтобы сделать атаки более трудоемкими: методы компиляции *XOR* с уникальными ключами шифрования, рандомизация *API* приложения и рандомизация структуры баз данных.

Динамическое изменение параметров сети (*dynamic network*), таких как используемые протоколы (включая протоколы маршрутизации), *IP*- и *MAC*-адреса, порты, алгоритмы шифрования, используемые для идентификации, а также маршруты передачи трафика (информационные направления).

Динамическое изменение среды выполнения (*dynamic runtime environment*), заключающееся в изменении среды выполнения, предоставленной приложению операционной системой, а именно – содержимого памяти (расположения программного кода, библиотек, стека, кучи и индивидуальных функций).

Динамическое изменение платформы (*dynamic platform*), которое заключается в изменении свойств аппаратного обеспечения (архитектуры процессора, памяти, формата данных платформы) и операционной системы (ее типа и версии).

Таким образом, при реализации концепции *MTD* защита ИС в условиях ведения злоумышленником КР и КА должна основываться не на обнаружении, а на предотвращении несанкционированных (деструктивных) воздействий.

В рамках маскирования структуры распределенных информационных систем в киберпространстве направлениями первоочередной разработки являются (см. рис. 2):

- динамическое изменение параметров сети (маскирование информационных направлений распределенных ИС и динамическое управления сетевым адресным пространством);
- динамическое изменение платформы (проактивная защита внутренней структуры ИС).

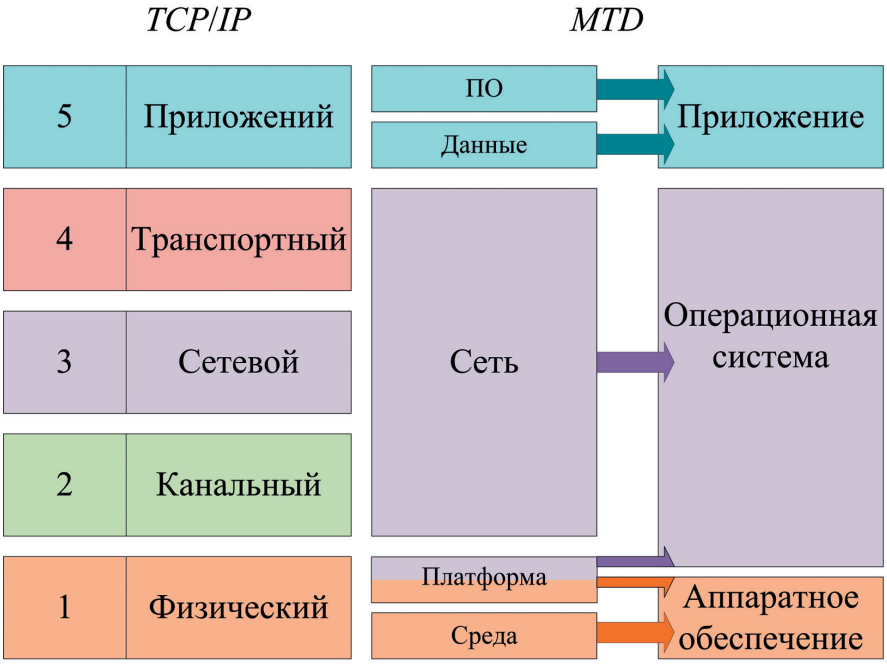

Рис. 1. Направления подхода MTD в контексте модели TCP/IP

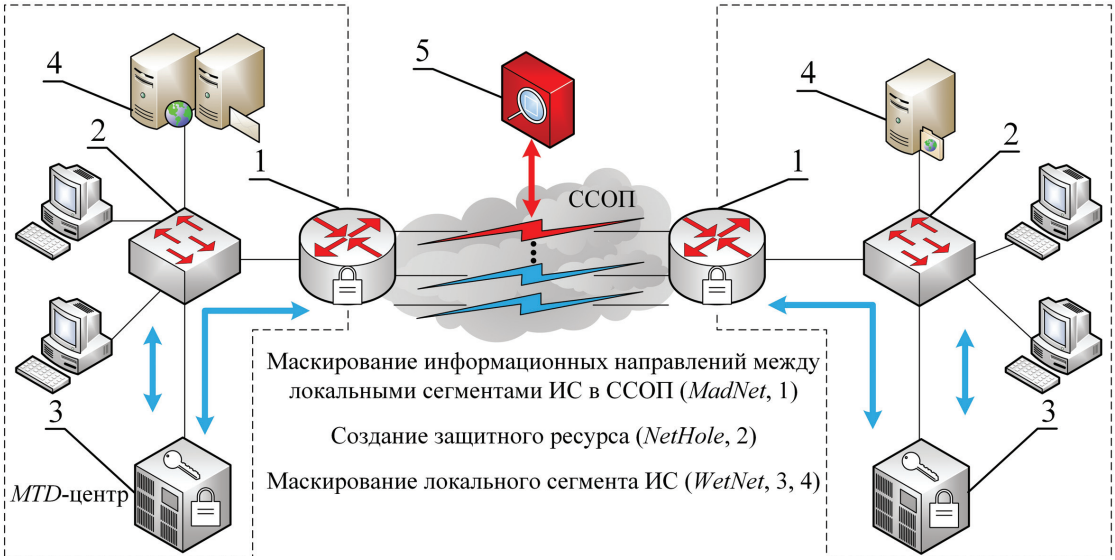

Рис. 2. Место технических средств маскирования в структуре распределенной ИС (на примере интеграции двух локальных сегментов ИС)

5. Маскирование информационных направлений

В рамках динамического изменения параметров сети, разработан ряд способов маскирования структуры сети связи [9-11], которые обеспечивают повышение защищенности информационных направлений (ИН) ИС от КР и КА. Способы реализованы в виде программного средства *MadNet* – маскиратора информационных направлений ИС (далее – маскиратор), который расширяет возможности сетевого стека операционных систем семейства *GNU/Linux*.

Маскиратор позволяет обеспечить защиту функционально-логической структуры ИС при передаче информации по каналам связи, имеющим выход за пределы контролируемой зоны, путем сокрытия реальных направлений информационного обмена в общем объеме трафика, циркулирующего между распределенными сегментами ИС [12, 13]. В результате сетевые идентификаторы (*IP*- и *MAC*-адреса) в перехваченных пакетах сообщений нельзя поставить в соответствие конкретному коммуникационному узлу защищаемой ИС, что снижает возможности КР по реконструкции структуры и КА на элементы ИС.

Маскиратор (выноска № 1 на рис. 2) обеспечивает согласованное динамическое изменение идентификаторов коммуникационных узлов (*IP*- и *MAC*-адресов, а также номеров портов в заголовках пакетов сообщений), функционирующих в *VPN*, при этом не является разновидностью известных техник изменения сетевых адресов. В результате маскирования вместо одного информационного направления злоумышленнику (выноска № 5 на рис.2) для анализа предоставляется заранее заданная конфигурационным файлом ложная структура, которая характеризуется совокупностью маскированных ИН (передают конструктивный трафик) и маскирующих ИН (обеспечивают ложный фон). Ложная структура поддерживается с помощью генерации произвольного трафика, объем которого уменьшают пропорционально увеличению объема конструктивного трафика, при этом задают степень утилизации каждого маскирующего ИН [14, 15].

Включение маскиратора в структуру ИС позволит обеспечить:

- ослабление влияния или нейтрализацию системы КР и КА злоумышленника за счет снижения доступности элементов ИС и процессов управления;
- лишение злоумышленника необходимой информации о структуре распределенной ИС, или затруднение анализа информации за счет снижения информативности ДМП и процессов управления;
- формирование ложных стереотипов относительно информационных направлений ИС, составе элементов ИС, функционально-логической структуре ИС и алгоритмах ее функционирования за счет навязывания ложной информации о структуре ИС и процессах управления.

6. Динамическое управление сетевым адресным пространством

Для защиты внутренней структуры ИС в рамках динамического изменения параметров сети достаточно широко применяются методы киберманеврирования (*cyber maneuvering*) [16]. Киберманеврирование заключается в периодическом (синхронизированном по времени) или неуправляемом (случайном) изменении сетевых настроек абонентов внутри ИС (используемого адресного пространства и номеров портов абонентов), например с использованием методов *NASR* (*Network Address Space Randomization*) и *RHM* (*Random Host*

Mutation) [8]. При технической реализации киберманеврирования применяется *DHCP*-сервер с расширенными настройками, обеспечивающий синхронизацию по времени сетевых параметров или обмен служебными пакетами сообщений об алгоритме изменения этих параметров при наступлении заданного события безопасности. Синхронизация адресного пространства между абонентами и разделяемыми информационными ресурсами ИС достигается внесением изменений в конфигурацию *DNS*-сервера.

Недостатками известных технических решений, реализующих киберманеврирование являются: узкая область применения, обусловленная частой автоматической сменой сетевых параметров абонентов, что повышает вероятность компрометации применяемого средства и раскрытия алгоритма изменения сетевых параметров; низкая результативность, обусловленная ограничением на изменение используемого адресного пространства в пределах одной (действующей) подсети.

В рамках динамического изменения параметров сети разработан ряд способов защиты ИС от КР, которые устраняют указанные недостатки. Способы реализованы в виде программного комплекса проактивной защиты ИС от КР WetNet на основе динамического управления сетевым адресным пространством.

Управление сетевыми параметрами абонентов в программном средстве WetNet (выноска № 3 на рис.2) осуществляется путем принудительного изменения IP-адресов абонентов DHCP-сервером и динамического изменения портов информационных ресурсов ИС при обнаружении подозрительной сетевой активности. Это позволяет снизить вероятность компрометации представленного программного средства и исключить возможность идентификации злоумышленником алгоритма изменения сетевых параметров.

Низкая результативность аналогов, обусловленная ограничением на изменение используемого адресного пространства в пределах одной подсети, устраняется в программном средстве WetNet использованием для маневрирования нескольких подсетей.

Разработанное техническое решение уменьшает длительность времени в течение которого информация, полученная в результате ведения КР, будет достоверной, а также увеличивает необходимый злоумышленнику ассортимент средств КР и количество операций сканирования. Указанные преимущества способствуют компрометации средств КР злоумышленника.

7. Проактивная защита структуры локальных сегментов ИС

В рамках динамического изменения платформы активное распространение получили сетевые приманки (*honeypots*), которые предназначены для формирования у злоумышленника ложных стереотипов относительно количества и типологии уязвимых целей в структуре локальных сегментов ИС и, соответственно, способствуют навязыванию ему более сложной (избыточной) структуры ИС [1, 17-19].

Одной из разновидностей сетевых приманок являются такие средства сетевого обмана, как сетевые ловушки (*network tarpits*) [20], которые не только предъявляют злоумышленнику ложную структуру ИС, но и способны взаимодействовать с его системами КР и КА, например, принудительно удерживать несанкционированные соединения, что приводит к «истощению» вычислительных ресурсов злоумышленника, и (или) замедлять процесс автоматического сетевого сканирования, вынуждая злоумышленника расходовать избыточный ресурс для реализации целей КР.

В свою очередь, злоумышленниками активно разрабатываются и совершенствуются средства компрометации сетевых ловушек. Анализ исследований в данной предметной области показал, что сетевым ловушкам присущи ДМП, которые характеризуются [20]:

- использованием строго заданных идентификаторов коммуникационных узлов;
- использованием отличительных параметров (опций) протоколов стека *TCP/IP*.

ДМП первого типа является использование единственного и неизменяемого значения *MAC*-адреса при ответах на *ARP*-запросы (например, адрес *00:00:0F:FF:FF:FF* используется в ловушке *LaBrea*) независимо от реального адреса сетевого адаптера.

ДМП второго типа выявляются при детальном анализе сетевого трафика, поступающего от сетевых ловушек, а компрометирующими факторами в этом случае являются характерные значения служебных полей «Размер окна» и «Опции» в *TCP*-заголовке, ответы на сетевые запросы, демонстрирующие доступность (активность) всего адресного пространства и пространства используемых сетевых портов, а также отсутствие характерных ответов на сетевые запросы при использовании протоколов уровня приложений (*FTP*, *HTTP* и других).

В качестве средств компрометации сетевых ловушек применяются как известные сетевые утилиты различных типов (*Nmap*, *Ethereal*, *Arping*, *Wireshark*, *«Сканер-ВС»*), так и специализированные утилиты (*Honeypot Hunter*, *Honeypot Killer, Degreaser*).

В рамках динамического изменения платформы разработан ряд способов устранения ДМП, присущих сетевой ловушке *LaBrea*, повышения результативности ее функционирования [21, 22], и направленных на снижение вероятности ее идентификации (компрометации мер защиты). Способы реализованы в виде программного комплекса проактивной защиты вычислительных сетей *NetHole*.

Для снижения вероятности компрометации сетевой ловушки в программном средстве *NetHole* (выноска № 2 на рис.2) реализованы следующие конструктивные преимущества: рандомизация значений *MAC*-адресов сетевых адаптеров; управление значениями полей «Размер окна» и «Опции» *TCP*-заголовка; генерация ответов на сетевые запросы уровня приложений; разделение пространства *IP*-адресов и пространства используемых сетевых портов на виртуальные области. Указанные преимущества обеспечивают реалистичность сетевого обмана и бескомпроматность мер защиты [23, 24].

Удержание соединения в сетевой ловушке *LaBrea* реализовано за счет использования нулевого значения

поля «Размер окна» *TCP*-заголовка после установления соединения. Для увеличения времени удержания соединения в программном комплексе *NetHole* дополнительно реализована возможность имитации канала связи с плохим качеством за счет повторной отправки пакетов сообщений с установленным флагом *ACK* в *TCP*-заголовке.

Для навязывания ложной внутренней структуры ИС в программном средстве *NetHole* реализованы следующие возможности: имитация различных типов коммуникационного оборудования (выноска № 4 на рис.2) путем назначения им ролей (сервер, маршрутизатор, коммутатор) и их количества; формирование ложных «отпечатков» (*fingerprints*) операционных систем имитируемых узлов.

Таким образом, в разработанном техническом решении достигается: скрытие факта и типологии используемых средств защиты за счет снижения вероятности обнаружения использования сетевых ловушек; повышение результативности защиты за счет увеличения времени, затрачиваемого злоумышленником на сетевое сканирование и редукцию результатов КР; введение злоумышленника в заблуждение относительно истинного состава и внутренней структуры (структуры локальных сегментов) защищаемой ИС.

Выводы

Анализ известных технических решений по маскированию структуры распределенных ИС в киберпространстве позволяет сформулировать основные цели маскирования:

- обеспечить скрытое управление путем формирования у злоумышленника устойчивых ложных стереотипов относительно форм, способов и приемов организации управления;
- реализовать управление ДМП функционально-логической структуры распределенных ИС, обеспечивающее затруднение идентификации абонентов сети и истинной структуры ИС несанкционированными абонентами;
- реализовать введение ложных элементов ИС путем расширения адресного пространства уже существующих элементов, изменения интенсивности информационных потоков с использованием маскирующего обмена и введения ложных информационных связей между элементами системы управления; устранения корреляции между структурами системы управления и ИС на информационном пространстве КР.

Принципы, заложенные в основу функционирования разработанных технических решений, реализуют направления динамического изменения параметров сети и динамического изменения платформы концепции *Moving Target Defense*.

Так, маскиратор информационных направлений ИС позволяет обеспечить сокрытие реальных направлений информационного обмена в общем объеме трафика, циркулирующего между распределенными сегментами ИС. В результате маскирования информационных направлений ИС вместо одного информационного направления злоумышленнику для анализа предоставляется заранее заданная конфигурационным файлом ложная структура, которая характеризуется совокупностью маскируемых ИН (передают конструктивный трафик) и маскирующих (ложных) ИН. Ложная структура поддерживается с помощью генерации произвольного трафика, при этом задается степень утилизации каждого ложного информационного направления, которая снижается пропорционально росту конструктивного трафика.

Программный комплекс динамического управления сетевым адресным пространством позволяет обеспечить сокрытие сетевых настроек абонентов ИС (используемого адресного пространства и номеров портов абонентов). Управление сетевыми параметрами абонентов осуществляется путем принудительного изменения времени аренды *IP*-адресов на *DHCP*-сервере и динамическим изменением сетевых портов информационных ресурсов ИС при обнаружении подозрительной сетевой активности. Синхронизация адресного пространства между абонентами и разделяемыми информационными ресурсами ИС осуществляется прозрачно (абоненту не нужно знать информацию об изменении сетевых параметров других абонентов ИС) для абонента и достигается внесением изменений в конфигурацию *DNS*-сервера.

Программный комплекс средств проактивной защиты [25] вычислительных сетей позволяет обеспечить сокрытие количества и характеристик уязвимых целей во внутренней структуре ИС и, соответственно, способствует навязыванию злоумышленнику более сложной (избыточной) структуры ИС, чем существующая. В разработанном техническом решении достигается: повышение результативности защиты и введение в заблуждение злоумышленника относительно структуры ИС, за счет снижения вероятности обнаружения факта использования средств проактивной защиты; увеличение времени автоматического сетевого сканирования; введение злоумышленника в заблуждение относительно истинного состава и внутренней структуры защищаемой ИС; повышение сложности и продолжительности анализа результатов КР.

Таким образом, при совместном использовании разработанных технических решений обеспечивается навязывание злоумышленнику ложной функционально-логической структуры ИС путем предъявления компьютерной разведке совокупности ДМП, характеризующей как внутреннюю, так и внешнюю структуру. В результате злоумышленник будет вынужден принимать решения в условиях неопределенности обстановки, а планы управления и технологические процессы будут искажены либо скрыты.

Литература:

1. Марков А.С., Цирлов В.Л. Руководящие указания по кибербезопасности в контексте ISO 27032 // Вопросы кибербезопасности. 2014. № 1(2). С. 28-35. DOI: 10.21681/2311-3456-2014-1-28-35
2. Климов С.М. Имитационные модели испытаний критически важных информационных объектов в условиях компьютерных атак // Известия ЮФУ. Технические науки. 2016. № 8 (181). С. 27-36.
3. Dorofeev A.V., Rautkin Y.V. Applied Aspects of Security Testing. In CEUR Workshop Proceedings, 2017, Vol-2081 (Selected Papers of the VIII All-Russian Scientific and Technical Conference on Secure Information Technologies, BIT 2017). P. 49-53.
4. Соколовский С.П., Шарифуллин С.Р., Чернолес В.П., Максимов Р.В. Инновационные информационные технологии в контексте обеспечения национальной безопасности государства // Инновации. 2018. №3 (233). С. 28-35.
5. Максимов Р.В., Иванов И.И. Этюды технологии маскирования функционально-логической структуры информационных систем / Инновационная деятельность в Вооруженных Силах Российской Федерации: Труды всеармейской научно-практической конференции. 11-12 октября 2017 года. – СПб.: ВАС, 2017 – 358с.
6. Меньшаков Ю.К. Теоретические основы технических разведок: Учеб. пособие / Под ред. Ю.Н. Лаврухина. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2008. – 536 с.: ил.
7. Марков А., Фадин А. Конвергенция средств защиты информации // Защита информации. Инсайд. 2013. № 4 (52). С. 80-81.
8. Sokolovsky S.P., Telenga A.P., Voronchikhin I.S. Moving Target Defense for Securing Distributed Information Systems // Информатика: проблемы, методология, технологии. Сборник материалов XIX международной научно-методической конференции / под ред. Д.Н. Борисова. – Воронеж.: ВГУ, 2019. С. 639-643.
9. Способ маскирования структуры сети связи. Патент 2656839 Российская Федерация, МПК G06F / Максимов Р.В., Иванов И.И., Лыков Н.Ю., Шарифуллин С.Р. и др. ; заявитель и патентообладатель Краснодарское высшее военное училище (RU). – № 2017114782; заявл. 26.04.2017; опубл. 06.06.2018, Бюл. № 16.
10. Способ маскирования структуры сети связи. Патент 2668979 Российская Федерация, МПК G06F / Максимов Р.В., Голуб Б.В., Лыков Н.Ю., Краснов В.А. и др.; заявитель и патентообладатель Краснодарское высшее военное училище (RU). – № 2017110366; заявл. 28.03.2017; опубл. 28.09.2018, Бюл. № 28.
11. Способ маскирования структуры сети связи. Патент 2645292 Российская Федерация, МПК H04L / Максимов Р.В., Иванов И.И., Шарифуллин С.Р., Мирошниченко Е.Л. и др.; заявитель и патентообладатель Краснодарское высшее военное училище (RU). – № 2016124953; заявл. 21.06.2016; опубл. 26.12.2017, Бюл. № 36.
12. Iskolnyy B.B., Maximov R.V., Sharifullin S.R. Survivability Assessment of Distributed Information and Telecommunication Networks // Selected Papers of the VIII All-Russian Conference with International Participation «Secure Information Technologies» (BIT 2017). Bauman Moscow Technical University. December 6-7, 2017, Moscow, Russia. P. 59-65.
13. Maximov R.V., Ivanov I.I., Sharifullin S.R. Network Topology Masking in Distributed Information Systems // Selected Papers of the VIII All-Russian Conference with International Participation «Secure Information Technologies» (BIT 2017). Bauman Moscow Technical University. December 6-7, 2017, Moscow, Russia. P. 83-87.
14. Максимов Р.В., Лыков Н.Ю., Шарифуллин С.Р. Маскирование структуры и алгоритмов функционирования интегрированных инфокоммуникационных систем // Технические и технологические системы. Сборник трудов VIII Международной научно-практической конференции «ТТС-16». – Краснодар, 2016. С. 203-206.
15. Максимов Р.В., Шерстобитов Р.С., Шарифуллин С.Р. Маскирование интегрированных сетей связи ведомственного назначения // Системы управления, связи и безопасности. 2018. № 4. С. 136-175.
16. Beraud, P., Cruz, A., Hassell, S., & Meadows, S. (2011). Using cyber maneuver to improve network resiliency. 2011 - MILCOM 2011 Military Communications Conference, 1121-1126.
17. Вишневский А.С. Обманная система для выявления хакерских атак, основанная на анализе поведения посетителей веб-сайтов // Вопросы кибербезопасности. 2018. № 3 (27). С. 54-62.
18. Шматова Е.С. Выбор стратегии ложной информационный системы на основе модели теории игр // Вопросы кибербезопасности. 2015. № 5 (13). С. 36-40.
19. Язов Ю.К., Сердечный А.Л., Шаров И.А. Методический подход к оцениванию эффективности ложных информационных систем // Вопросы кибербезопасности. 2014. № 1 (2). С. 55-60.
20. Maximov R.V., Sokolovsky S.P., Gavrilov A.L. Hiding Computer Network Proactive Security Tools Unmasking Features. In CEUR Workshop Proceedings, 2017, Vol-2081 (Selected Papers of the VIII All-Russian Scientific and Technical Conference on Secure Information Technologies, BIT 2017). P. 88-92.
21. Способ защиты вычислительных сетей. Патент 2680038 Рос. Федерация, МПК G06F / Максимов Р.В., Орехов Д.Н., Соколовский С.П., Гаврилов А.Л. и др.; заявитель и патентообладатель Краснодарское высшее военное училище (RU). – № 2018101596; заявл. 16.01.2018; опубл. 14.02.2019, Бюл. № 5.
22. Способ защиты вычислительных сетей. Патент 2649789 Рос. Федерация, МПК G06F / Максимов Р.В., Орехов Д.Н., Соколовский С.П., Проскуряков И.С.; заявитель и патентообладатель Краснодарское высшее военное училище (RU). – № 2017125677; заявл. 17.07.2017; опубл. 04.04.2018, Бюл. № 10.
23. Способ защиты вычислительных сетей. Патент 2682432 Рос. Федерация, МПК G06F / Максимов Р.В., Орехов Д.Н., Соколовский С.П., Крупенин А.В.; заявитель и патентообладатель Краснодарское высшее военное училище (RU). – № 2018110755; заявл. 26.03.2018; опубл. 19.03.2019, Бюл. № 8.

24. Способ защиты вычислительных сетей. Патент 2686023 Рос. Федерация, МПК G06F / Максимов Р.В., Орехов Д.Н., Соколовский С.П., Пряхин В.П. и др.; заявитель и патентообладатель Краснодарское высшее военное училище (RU). – № 2018120288; заявл. 31.05.2018; опубл. 23.04.2019, Бюл. № 12.
25. Соколовский С.П., Орехов Д.Н. Концептуализация проблемы проактивной защиты интегрированных информационных систем // Сборник научных статей VIII Международной научно-практической конференции «Научные чтения имени профессора Н.Е. Жуковского». – Краснодар: Издательский Дом – Юг, 2018. С. 47–52.

MASKING OF DISTRIBUTED INFORMATION SYSTEMS STRUCTURE IN CYBER SPACE

Voronchikhin I.S.[7],Ivanov I.I.[8], Maximov R.V.[9], Sokolovsky S.P.[10]

While formulating their requirements for information security, regulatory authorities require that security threats shall be defined considering the structural and functional characteristics of the information system including the information system structure and composition, physical, logical, functional, and technological relationships among the information system segments, applied information technologies and their operational peculiarities. The main protection measures suggested include the emulation of false components of the information systems, concealing real information technologies, information system configuration management and its transition to a preliminary defined configuration that ensures security. However, for a number of reasons, these measures are not included in the basic set of features, and the security goals are achieved by compensatory means such as formalization and implementation of prohibitive regulations and a complex of organizational and technical activities aimed to address the source of threat.

The purpose of the study is to reveal and formulate priority directions for searching of new technical solutions required to mask the structure of distributed information systems in cyber space thus removing the antagonism between the attacking and the defending parties.

The research method is based on obfuscation of the information system composition, structure, and operation mechanisms in cyber space. The formulated principles and developed masking technologies have been described using the terminology specific for the Moving Target Defense concept.

The outcome of the study includes an assortment of technical solutions used to mask information systems integrated into the public communication network. The obtained results allow open realization of protective measures aimed to create stable erroneous stereotypes relating to the information systems and management processes carried out on their basis.

Keywords: *cyber security, moving target defense, computer intelligence, information routes, proactive defense, network address space, false structure.*

References

1. Markov A.S., Cirlov V.L. Rukovodyashchie ukazaniya po kiberbezopasnosti v kontekste ISO 27032. Voprosy kiberbezopasnosti [Cybersecurity issues]. 2014. No 1(2), pp. 28-35. DOI: 10.21681/2311-3456-2014-1-28-35.
2. Klimov S.M. Imitacionnye modeli ispytanij kriticheski vazhnyh informacionnyh ob"ektov v usloviyah komp'yuternyh atak. Izvestiya YUFU. Tekhnicheskie nauki. – 2016. – No 8 (181). – S. 27-36.
3. Dorofeev A.V., Rautkin Y.V. Applied Aspects of Security Testing. In CEUR Workshop Proceedings, 2017, Vol-2081 (Selected Papers of the VIII All-Russian Scientific and Technical Conference on Secure Information Technologies, BIT 2017). P. 49-53.
4. Sokolovskij S.P., SHarifullin S.R., CHernoles V.P., Maksimov R.V. Innovacionnye informacionnye tekhnologii v kontekste obespecheniya nacional'noj bezopasnosti gosudarstva. Innovacii. 2018. No3 (233) , pp.28-35.
5. Maksimov R.V., Ivanov I.I. Etyudy tekhnologii maskirovaniya funkcional'no-logicheskoj struktury informacionnyh sistem / Innovacionnaya deyatel'nost' v Vooruzhennyh Silah Rossijskoj Federacii: Trudy vsearmejskoj nauchno-prakticheskoj konferencii. 11-12 oktyabrya 2017 goda. – SPb.: VAS, 2017 – 358s.

7 Ivan Voronchikhin, Postgraduate, Krasnodar Higher Military School, Krasnodar. Russia. E-mail: 5.00@mail.ru
8 Ilya Ivanov, Researcher, Krasnodar Higher Military School, Krasnodar. Russia. E-mail: 7570745@mail.ru
9 Roman Maximov, Dr.Sc., Professor, Krasnodar Higher Military School, Krasnodar. Russia. E-mail: rvmaxim@yandex.ru
10 Sergey Sokolovsky, Ph.D., Assistant Professor, Krasnodar Higher Military School, Krasnodar. Russia. E-mail: ssp.vrn@mail.ru

6. Men'shakov YU.K. Teoreticheskie osnovy tekhnicheskih razvedok: Ucheb. posobie / Pod red. YU.N. Lavruhina. – M.: Izd-vo MGTU im. N.E. Baumana, 2008. – 536 s.: il.
7. Markov A., Fadin A. Konvergenciya sredstv zashchity informacii. Zashchita informacii. Insajd. 2013. No 4 (52) , pp.80-81.
8. Sokolovsky S.P., Telenga A.P., Voronchikhin I.S. Moving Target Defense for Securing Distributed Information Systems. Informatika: problemy, metodologiya, tekhnologii. Sbornik materialov XIX mezhdunarodnoj nauchno-metodicheskoj konferencii. pod red. D.N. Borisova. – Voronezh.: VGU, 2019 , pp.639-643.
9. Sposob maskirovaniya struktury seti svyazi. Pat. 2656839 Rossijskaya Federaciya, MPK G06F / Maksimov R.V., Ivanov I.I., Lykov N.YU., SHarifullin S.R. i dr. ; zayavitel' i patentoobladatel' Krasnodarskoe vysshee voennoe uchilishche (RU). – No 2017114782; zayavl. 26.04.2017; opubl. 06.06.2018, Byul. No 16.
10. Sposob maskirovaniya struktury seti svyazi. Pat. 2668979 Rossijskaya Federaciya, MPK G06F / Maksimov R.V., Golub B.V., Lykov N.YU., Krasnov V.A. i dr.; zayavitel' i patentoobladatel' Krasnodarskoe vysshee voennoe uchilishche (RU). – No 2017110366; zayavl. 28.03.2017; opubl. 28.09.2018, Byul. No 28.
11. Sposob maskirovaniya struktury seti svyazi. Pat. 2645292 Rossijskaya Federaciya, MPK H04L / Maksimov R.V., Ivanov I.I., SHarifullin S.R., Miroshnichenko E.L. i dr.; zayavitel' i patentoobladatel' Krasnodarskoe vysshee voennoe uchilishche (RU). – No 2016124953; zayavl. 21.06.2016; opubl. 26.12.2017, Byul. No 36.
12. Iskolnyy B.B., Maximov R.V., Sharifullin S.R. Survivability Assessment of Distributed Information and Telecommunication Networks. Selected Papers of the VIII All-Russian Conference with International Participation «Secure Information Technologies» (BIT 2017). Bauman Moscow Technical University. December 6-7, 2017, Moscow, Russia. P. 59-65.
13. Maximov R.V., Ivanov I.I., Sharifullin S.R. Network Topology Masking in Distributed Information Systems. Selected Papers of the VIII All-Russian Conference with International Participation «Secure Information Technologies» (BIT 2017). Bauman Moscow Technical University. December 6-7, 2017, Moscow, Russia. P. 83-87.
14. Maksimov R.V., Lykov N.YU., SHarifullin S.R. Maskirovanie struktury i algoritmov funkcionirovaniya integrirovannyh infokommunikacionnyh sistem. Tekhnicheskie i tekhnologicheskie sistemy. Sbornik trudov VIII Mezhdunarodnoj nauchno-prakticheskoj konferencii «TTS-16». – Krasnodar, 2016 , pp.203-206.
15. Maksimov R.V., SHerstobitov R.S., SHarifullin S.R. Maskirovanie integrirovannyh setej svyazi vedomstvennogo naznacheniya. Sistemy upravleniya, svyazi i bezopasnosti. 2018. No 4 , pp.136-175.
16. Beraud, P., Cruz, A., Hassell, S., & Meadows, S. (2011). Using cyber maneuver to improve network resiliency. 2011 - MILCOM 2011 Military Communications Conference, 1121-1126.
17. Vishnevskij A.S. Obmannaya sistema dlya vyyavleniya hakerskih atak, osnovannaya na analize povedeniya posetitelej veb-sajtov. Voprosy kiberbezopasnosti [Cybersecurity issues]. 2018. No 3 (27) , pp.54-62.
18. SHmatova E.S. Vybor strategii lozhnoj informacionnyj sistemy na osnove modeli teorii igr. Voprosy kiberbezopasnosti [Cybersecurity issues]. 2015. No 5 (13) , pp.36-40.
19. YAzov YU.K., Serdechnyj A.L., SHarov I.A. Metodicheskij podhod k ocenivaniyu effektivnosti lozhnyh informacionnyh sistem. Voprosy kiberbezopasnosti [Cybersecurity issues]. 2014. No 1 (2) , pp.55-60.
20. Maximov R.V., Sokolovsky S.P., Gavrilov A.L. Hiding Computer Network Proactive Security Tools Unmasking Features. In CEUR Workshop Proceedings, 2017, Vol-2081 (Selected Papers of the VIII All-Russian Scientific and Technical Conference on Secure Information Technologies, BIT 2017). P. 88-92.
21. Sposob zashchity vychislitel'nyh setej. Pat. 2680038 Ros. Federaciya, MPK G06F / Maksimov R.V., Orekhov D.N., Sokolovskij S.P., Gavrilov A.L. i dr.; zayavitel' i patentoobladatel' Krasnodarskoe vysshee voennoe uchilishche (RU). – No 2018101596; zayavl. 16.01.2018; opubl. 14.02.2019, Byul. No 5.
22. Sposob zashchity vychislitel'nyh setej. Pat. 2649789 Ros. Federaciya, MPK G06F / Maksimov R.V., Orekhov D.N., Sokolovskij S.P., Proskuryakov I.S.; zayavitel' i patentoobladatel' Krasnodarskoe vysshee voennoe uchilishche (RU). – No 2017125677; zayavl. 17.07.2017; opubl. 04.04.2018, Byul. No 10.
23. Sposob zashchity vychislitel'nyh setej. Pat. 2682432 Ros. Federaciya, MPK G06F / Maksimov R.V., Orekhov D.N., Sokolovskij S.P., Krupenin A.V.; zayavitel' i patentoobladatel' Krasnodarskoe vysshee voennoe uchilishche (RU). – No 2018110755; zayavl. 26.03.2018; opubl. 19.03.2019, Byul. No 8.
24. Sposob zashchity vychislitel'nyh setej. Pat. 2686023 Ros. Federaciya, MPK G06F / Maksimov R.V., Orekhov D.N., Sokolovskij S.P., Pryahin V.P. i dr.; zayavitel' i patentoobladatel' Krasnodarskoe vysshee voennoe uchilishche (RU). – No 2018120288; zayavl. 31.05.2018; opubl. 23.04.2019, Byul. No 12.
25. Sokolovskij S.P., Orekhov D.N. Konceptualizaciya problemy proaktivnoj zashchity integrirovannyh informacionnyh sistem. Sbornik nauchnyh statej VIII Mezhdunarodnoj nauchno-prakticheskoj konferencii «Nauchnye chteniya imeni professora N.E. ZHukovskogo». – Krasnodar: Izdatel'skij Dom – YUg, 2018 , pp.47–52.