УМНАЯ БОТ-СЕТЬ ИЛИ МОДЕЛЬ ИНТЕЛЛЕКТУАЛЬНОГО ДЕСТРУКТОРА

Рыженко А.А.[1]

Целью работы *является разработка модели интеллектуального деструктора бот-сети, содержащей автономные и полуавтономные ресурсы.*

Метод исследования: *методы мультимножества, концептуальное моделирование, алгоритмизация процессов.*

Результат исследования: *разработана модель формирования правил перехода состояний интеллектуальных деструкторов единой сети как автономного элемента и как части единой сети одновременно. Особенностью модели является адаптивность к внешним возмущениям за счет использования агентной модели методологии системы систем и семантики связей между ними с использованием единого неразрушимого ядра базы правил и множественного выбора древовидной иерархии поля решений баз ассоциаций. Правила продукционного типа представлены в упрощенной алгебраической форме по аналогии с современными алгоритмами построения цифровой подписи (организация зоны доверия с открытыми ключами). Полученная постановка решает такую проблему, как появление естественным образом отшельников и изгой в виде однозадачных автонов, что являлось одной из ключевых проблем полиморфных деструкторов.*

Научная новизна *заключается в разработке нового элемента концептуального моделирования деструкторов моделей – атрибутивного процесса, позволяющего адаптивно изменять правила перехода состояний.*

Ключевые слова: *деструктор, моделирование, интеллектуальный агент, фасет, иерархия, правила перехода, автоном, поле решений, полиморфик.*

DOI:10.21681/2311-3456-5-60-68

Введение

Многолетний анализ сводных отчетов и примеров утечек информации и атак на информационные ресурсы всемирной сети Интернет из новостных лент (дайджестов) показывает, что организуемые и используемые для деструктивного воздействия бот-сети вполне организованны и управляемы многоуровневой иерархической распределенной сетью с одним аналитическим центром (ядро системы) [1]. Общая модель управляемого деструктора аналогична модели конструктора информационного обмена, используемого поисковыми системами, но есть ряд особенностей, о чем и будет рассмотрено в статье. Раннее в некоторых публикациях поднималась данная тематика, но целевой модели так и не было обнаружено [2].

Стоит сразу отметить, что данная технология не нова, развитие продолжается десятилетиями, о чем свидетельствует неофициальная статистика одного из направлений социальной инженерии [3]. Отслеживаемые заказные атаки второго и третьего уровня (организованные средними группами и уровнем экспертов взломщиков) начиная с 90-х годов прошлого века показывают, насколько организованная сеть атакующих способна достаточно долго обрабатывать заказанного клиента любого уровня защищенности для достижения итоговой цели (обрушение, кража, подлог информации и т. п.). Данная особенность сформировала новое направление взлома – однозадачные ловушки деструкторов. Первое десятилетие 2000-х годов показало, что благодаря данным разработкам организованность атакующих начала плавно переходить от групповых атак с привлечением взломщиков к атакам с использованием автономных и полуавтономных сетей ловушек или бот-сетей. Данная тенденция породила новое направление развития интеллектуальных ботов деструкторов, способных не только автономно выполнять простые задачи на уровне вируса, но и также быть частью общей сети в нужный момент времени. Здесь уместно вспомнить алгоритм одного

1 Рыженко Алексей Алексеевич, кандидат технических наук, доцент, доцент департамента информационной безопасности, Финансовый университет при Правительстве РФ, г. Москва, Россия. E-mail: AARyzhenko@fa.ru

из самых эффективных деструкторов – алгоритм вируса полиморфик [4]. Многие публикации отметили, что данный алгоритм на примерах показывает, как в автономной сети в полуавтономном режиме может происходить эволюция программного кода, что дает основу для интеллектуальных систем деструкторов [5].

Официальная статистика выявленных попыток расставить боты-ловушки в сети Интернет со встроенным однозадачным алгоритмом для последующего деструктивного действия показали, насколько данная идея способна жить, развиваться и показывать результаты [6]. Примеры дайджестов, описывающих заказные атаки, основанные на исторических событиях разных государств (выборы государственных деятелей, реорганизация ключевых игроков глобального рынка, обрушение валюты государства или другого аналогичного рынка и т.д.) показывают эффективность интеллектуальных агентов деструкторов. Также часто используются более простые атаки с использованием бот-сетей для банковских систем или других финансовых структур [7]. Отмечено, что все чаще используют программируемые бот-сети для массового информационного вброса в электронные средства информации [8]. Развитие мобильных систем связи и коммуникаций, а также систем с открытым кодом и *app*-приложений открыло второе дыхание для систем долгосрочного управления сетью деструкторов [9] и т.д.

Систематизация полученной информации позволила заложить и описать модель бот-сети интеллектуального деструктора. Рассмотрим разработанную модель более подробно.

1. Обобщенное описание разрабатываемой модели бот-сети деструктора

Классическая теория управления включает множество компонентов взаимосвязанных между собой различных систем поддержки управления [10]. В основе связи элементов модели закладываются различные формы правил и ограничений. При переходе системы от простого уровня к комплексному устанавливается дополнительное условие: для дальнейшего развития системы помимо *конструктора* (порождающего новые объекты, процессы и потоки данных) должен использоваться *деструктор* ресурсов (уничтожающий временные структуры, коллизии, неиспользуемые архивы данных и т.д.). Для стабильного функционирования развивающейся системы ключевые задачи деструктора должны выполняться в полном объеме, иначе система начинает съедать себя изнутри, что приводит к эффекту самоуничтожения [11].

С другой стороны, информационные системы не всегда выполняют это требование, что связанно с ограничениями ресурсов в основном технической составляющей, т.е. деструктор также будет требовать ресурсы, а взять из негде. Например, самые популярные операционные системы внедрили первые деструкторы только в 2007 году при переходе на кроссплатформенные технологии (например, интеллектуальная корзина). Данное событие напрямую связано с развитием технической составляющей. Аналогичная история и со всемирной сетью. Переход на оптоволоконную сеть и массовое развитие спутниковой (и сотовой) связи способствовало развитию деструктивной сети в целом. Как следствие, современные информационные потоки также способствовали развитию не только конструктивной составляющей, но и деструктивной. Самым популярным примером являются организованные массовые *DDoS*-атаки [12].

Стоить отметить развивающуюся тенденцию существующих систем защиты информации – необходимость моделирования не столько самой системы защиты, сколько модели деструктора, что в дальнейшем позволяет комплексным системам защиты информации динамично принимать своевременные решения при атаках различного типа. Ранее были представлены некоторые элементы модели в публикациях [13]. Дальнейшее развитие системы позволило синтезировать полученную информации и представить в виде единой модели. Разработанная модель базируется на трех теоретических составляющих:

- бикубическая матрица «*атакуемые ресурсы – методы атаки*» – используется матричный подход организации данных, где одна из осей каждой матрицы смежная, а вторая – содержит ключевые параметры для построения узловых точек поля решений;
- модифицированные правила перехода состояний системы – позволяют формировать простые правила базы ассоциаций, позволяющие переходить между узловыми точками по определенным правилам;
- динамическое дерево последовательности атак на ресурсы – временно формируемый иерархические структуры, позволяющие устанавливать связи между узловыми точками, а также уровни иерархии принятия решений.

Данные методы используются при построении моделей угроз для объектов информационной инфраструктуры многих организация в том или ином виде [14].

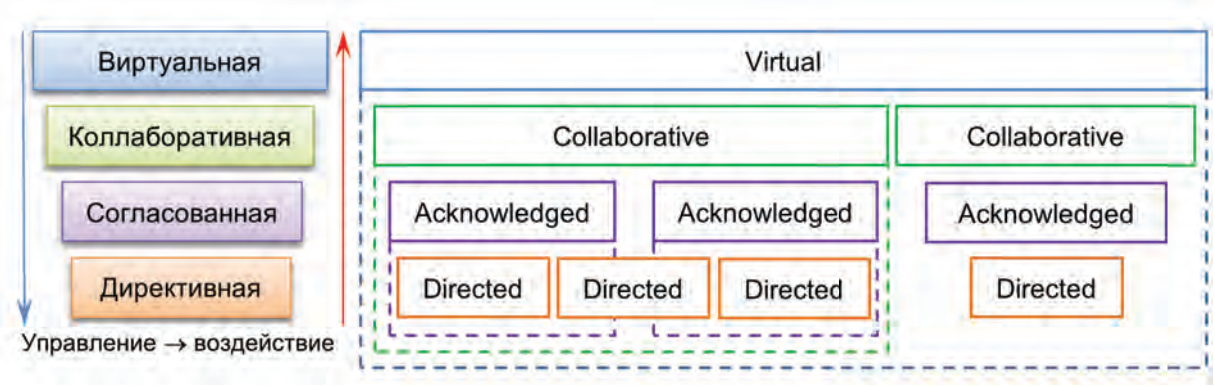

Рис. 1. Варианты иерархии «системы систем»

Приведенные выше составляющие имеют разный формат данных и разные формы построения ассоциативных правил. Анализ возможных форм взаимодействия выявил, что предлагаемый разными моделями онтологий системы взаимодействия не позволяют описывать процессные модели данных, что вызывает ряд вопросов в отношении универсальности предлагаемых разными авторами подходов [15]. Как следствие, для взаимосвязи неформатных данных выбрана для использования методология «*system of systems*» (*SoS*). Описание типов связей или процессов между элементами поля решений основано на следующей классификации *SoS*: виртуальная (*Virtual*), коллаборативная или мягкая (*Collaborative*), согласованная или смешанная (*Acknowledged*) и директивная или жесткая (*Directed*) [16]. Жесткие и смешанные системы позволяют собой условно управлять, что (опять же условно) может декларировать как более низкий (промежуточный) подкласс (рис. 1). Ранее в публикациях более подробно были рассмотрены данные подклассы[2].

Дальнейший анализ информационных источников не позволил выявить формального математического обоснования принципов организации *SoS*. Используемые на практике модели указывают, что необходимо применять дополнительные логические сценарии, позволяющие *одновременно работать и как часть целого и как само целое*, *пытаться «выжить» не управляя фактически ничем и никем*. Данный принцип (из зарубежных источников) получил название – *Russian babushka doll* или *Матрёшка*[3].

Подводя промежуточные итоги, можно сделать следующий вывод: существует множество технологий по заражению информационных ресурсов деструкторами (первый этап построения бот-сети), существуют методологии по организации управления бот-сетью для выполнения одной целевой задачи, также существуют методологии долгосрочного управления динамичной бот-сетью для решения пролонгируемых задач. Но единой теоретической модели, позволяющей не только слепо управлять бот-сетью, но и иметь встроенный инструмент анализа текущего состояния на практике не существует. В результате все чаще появляются такие автономные деструкторы как *изгои* и *отшельники*. Поведение данных категорий непредсказуемое, что доставляет ряд проблем как защищающимся, так и для самих атакующих злоумышленников и разработчиков в одном лице. Дальнейшее изложение материала будет как вариант решения данной задачи.

2. Теоретическая модель

Для формирования итоговой модели интеллектуального агента бот-сети произведена выборка из существующих теоретических подходов. В результате элемент структуры модели агента используется для:

- *матричное представление данных* – кортеж данных системы распределения ресурсов: динамические адреса источников деструкторов + задача автономного деструктора + алгоритм целевых воздействий деструктора. Располагаются в ячейках матрицы с активными границами;
- *иерархичное представление данных* – структурные древовидные алгоритмы последовательностей воздействий (атак) на информационные ресурсы. Привязано к матрице и фасету данных. В бикубической матрице является связующим звеном между кортежем данных и кортежем процессов;
- *сетевая структура данных* – условные алгоритмы возможных переходов состояний при целевых атаках на информационный ресурс. Позволяют анализировать не только общее состояние

2 Systems of Systems (SoS). URL: https://www.sebokwiki.org/wiki/Systems_of_Systems_(SoS) (дата обращения: 15.08.2023)

3 Molly Sharbach, Math enables custom arrangements of liquid “nesting dolls”. URL: https://engineering.princeton.edu/news/2020/11/30/math-enables-custom-arrangements-liquid-nesting-dolls (дата обращения: 15.08.2023)

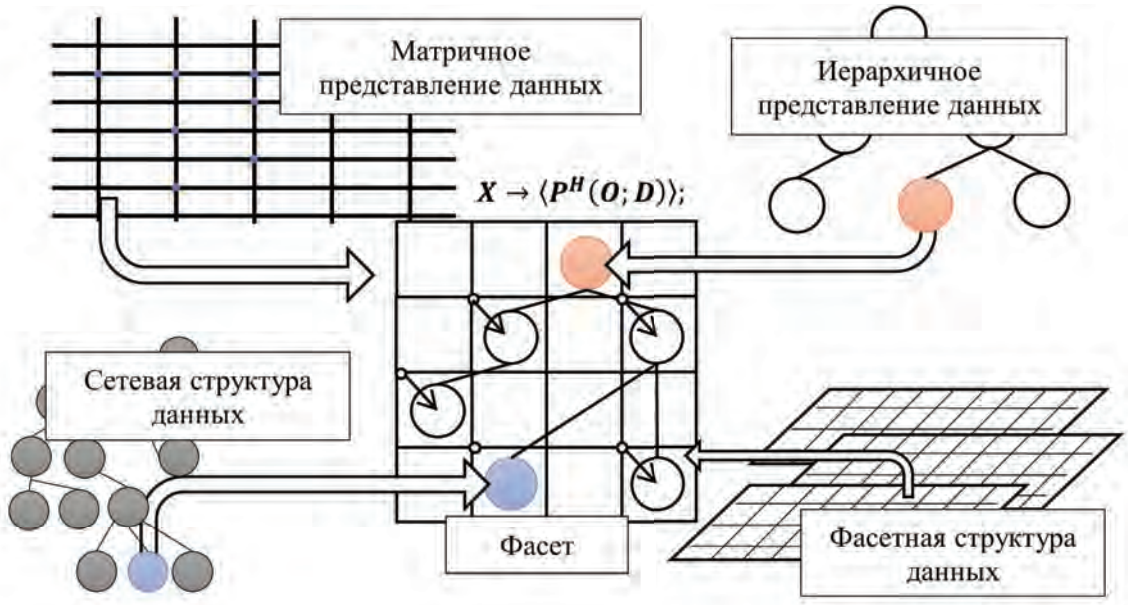

Рис. 2. Схематичное представление симбиоза используемых методологий

системы бот-сети, но и детализировать для каждого задействованного деструктора;

— *фасетная структура данных* – кортеж процессов системы распределения ресурсов: динамические адреса атакуемых ресурсов + исполняемые задачи деструкторов (например, вовремя *DoS*-атаки) + алгоритм изменения последующих ветвей иерархии данных в зависимости от текущего состояния. Используется формальная модель продукционного правила с нефиксированной правой частью.

Общее представление системы синтеза используемых в данной модели методологий представлено на рис. 2. Основной кортеж перехода состояний (1):

$$X \rightarrow P^H\left(O;D\right); \quad (1)$$

где:

X – *experience*, описание состояния системы бот-сети.

P^H – *hierarchical process*, иерархическая процессная составляющая, основанная на фасетной структуре данных.

O – *objects*, объектная составляющая, основанная на матричной структуре данных.

D – [*brain*] *data*, алгоритмическая составляющая – модель основного элемента поля решений интеллектуального агента.

Рассмотрим каждый компонент отдельно:

1. Матричное представление данных (бикубическая матрица «*атакуемые ресурсы – методы атаки*»). Для формирования одной границы смежности используется минимальное дуальное количество матриц, т. е. количество матриц ограничивается нижней границей равной двум. Одна матрица отвечает за динамическое распределение адресов источников деструкторов «*адрес источника – деструктор*», вторая – за адресную системы атакуемой цели «*деструктор – адрес цели*» (рис. 3).

Основная матрица перераспределения адресов *автономов* деструкторов располагается в ядре модели в базе правил (БП). Матрицы атакуемых ресурсов располагаются во временно создаваемых базах ассоциаций ($БА_i$). В чем принципиальной отличие комбинации «*база правил – базы комбинаций*» от «*базы знаний*» было подробно рассмотрено в публикациях на сторонних примерах [15]. Как было упомянуто ранее, взаимосвязь между ячейками матрицы происходит с использованием *алгоритмов последовательности атак*, подключается второй компонент – иерархическое дерево.

2. Динамическое дерево последовательности атак на ресурсы (рис. 4). Основные постулаты:

— *не существует заранее предопределенных унифицированных иерархий деревьев*. Достаточным условием является наличие правил переходов и правил разрешения простых коллизий. Эффект *метаморфа* позволяет конструировать иерархию деревьев на основе сетевой структуры за счет продукционных правил перехода состояний;

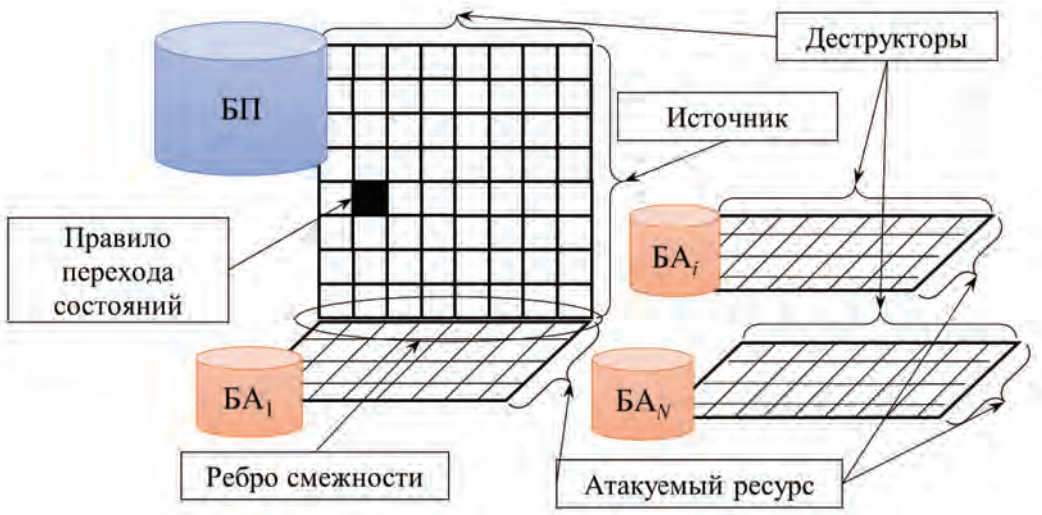

Рис. 3. Схематическое представление бикубической матрицы

— *не существует ограничений на количество уровней иерархии, минимальное количество ограничено базовым условием одноуровневого процесса*, т.е. минимальное количество уровней равно двум, что соответствует простой атаке деструктора;
— *первоначальное количество источников адресов деструкторов ограничивается одним условием – наличием минимум одной альтернативы, либо использованием отшельника в качестве источника*;
— *адрес каждого деструктора изгой заносится в отдельную матрицу без привязок к процессам*. Данная матрица также хранится в базе правил;
— *целевые ресурсы под постоянном мониторингом состояния осуществляются архитектором, анализ состояния не проводится*. Количество атакуемых ресурсов не может превышать количество источников с учетом временных ресурсов;
— *вариативные ресурсы используются для временного перехода в состояние источник до момента активной атаки, затем деструктор самоуничтожается (временный ресурс)* и т. д.

Количество первоначальных правил ровно 13, что соответствует количеству основных аксиом используемой в модели алгебры мультимножеств[4]. На рис. 4 не отражено, но параллельно с прямым деревом иерархии формируется обратное целевое дерево. Точки пересечения двух деревьев в узлах позволяют автономно конструировать набор исходных данных для правил перехода состояний.

3. Модифицированные правила перехода состояний системы. С одной стороны, в данной модели используется классическая форма продукционного правила, где элементами являются: описание класса ситуаций, условие, при котором продукция активизируется, ядро продукции и постусловие продукционного правила. Но, как было упомянуто ранее, в отличии от функционала конструктора, используется деструктивное свойство полиморфика. Ядро продукции не приводит к единому решению, а производит выборку вариантов решений в выделенном диапазоне. Более подробно данную особенность процессных моделей можно изучить в публикации [1]. Например, у узла дерева имеется максимально 5 источников, при этом атакуемых ресурсов всего 4. Количество атак на один ресурс не ограничено. Описать правило перехода ядра продукции для атаки из двух источников на один ресурс кортежа (1) можно следующим образом (2):

$$1+1\underset{5}{\rightarrow}[1;1..4] \qquad (2)$$

Вывод по теоретической части: представлен синтез теоретических подходов при формировании поля решений действий интеллектуального агента. Особенностью является использование модификаций правил продукционного типа в алгебраической форме в базе правил ядра разработанной модели, а также синтез ядра и множеств матриц атакуемых ресурсов баз ассоциаций. Алгебраическая форма представления ядра продукционного правила позволяет интеллектуальной части деструктора более оперативно принимать решения за счет искусственного устранения

4 Мультимножества. – режим доступа: https://life-prog.ru/1_47229_multimnozhestva.html (дата обращения: 15.08.2023)

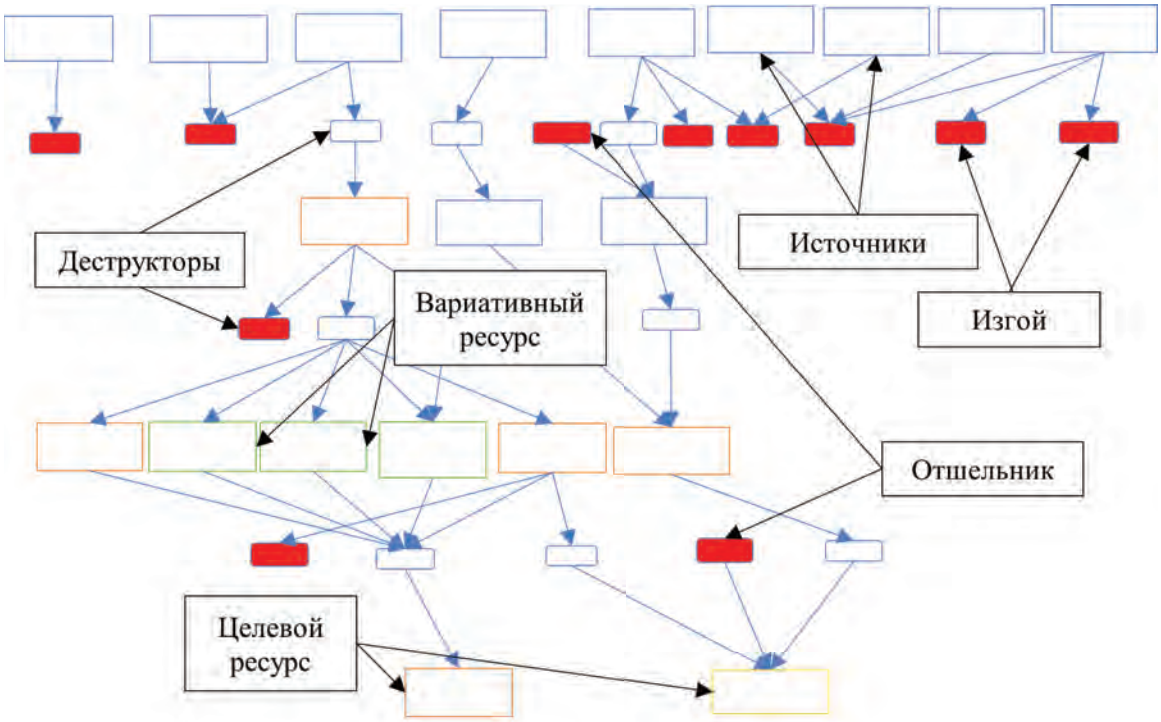

Рис. 4. Пример построения динамического дерева последовательности атак

источников парадоксов и коллизий. Вариативность альтернативных решений позволяет отрабатывать возможные сценарии, что приводит к однозначному решению.

3. Практические наработки

На рис. 5 представлен пример формирования поля решений деструктора с использованием шаблонов базы правил, а также сценариев баз ассоциаций. Для визуализации используем аффинную систему координат, где:

- ось абсцисс – ребро смежности между матрицами источников деструкторов и целевых атакуемых ресурсов;
- ось ординат – ребро смежности между матрицей целей и иерархией алгоритмов атак;
- ось аппликат – ребро смежности между матрицей источников и иерархией алгоритмов атак;

Для индикации состояний узловых точек используется классическая модель светофор: зеленый – успех, желтый – требуется действие, красный – неуспех. Организация мониторинга интеллектуальным деструкторов осуществляется через отклики автономов ботов следующим образом:

- *автоном деструктор с откликом* – после успешной атаки отправляет сигнал хозяину. Например, троян отправляет полученную информацию и меняет состояние индикатора или червь вносит изменения, отправляет запрос трояну и через посредника меняет состояние индикатора;
- *автоном деструктор без отклика* – однозадачный процесс, не отправляет хозяину отклик независимо от текущего состояния. Как правило данные автономы используются для массовых атак на информационные ресурсы и нет необходимости оперативного наблюдения;
- *полуавтоном деструктор с откликом* – деструктор наблюдатель. Данная категория не несет прямых деструктивных действий, но способствует атакам. Например, сканер портов, монитор активных потоков, монитор реестров, монитор файловой активности и т. д.;
- *полуавтоном деструктор без отклика* – деструктор посредник. Фактически выполняет роль поддержки управления для взломщиков. Проводит аудит системы на наличие поисковых механизмов обратного слежения потоков данных через сканеры портов, а также антивирусной активности в разных проявлениях. Работает совместно с предыдущими ботами в роли координатора и контролера. Готовых программных приложений для данной категории не существует. Каждая бот-сеть готовит данную категорию уникально.

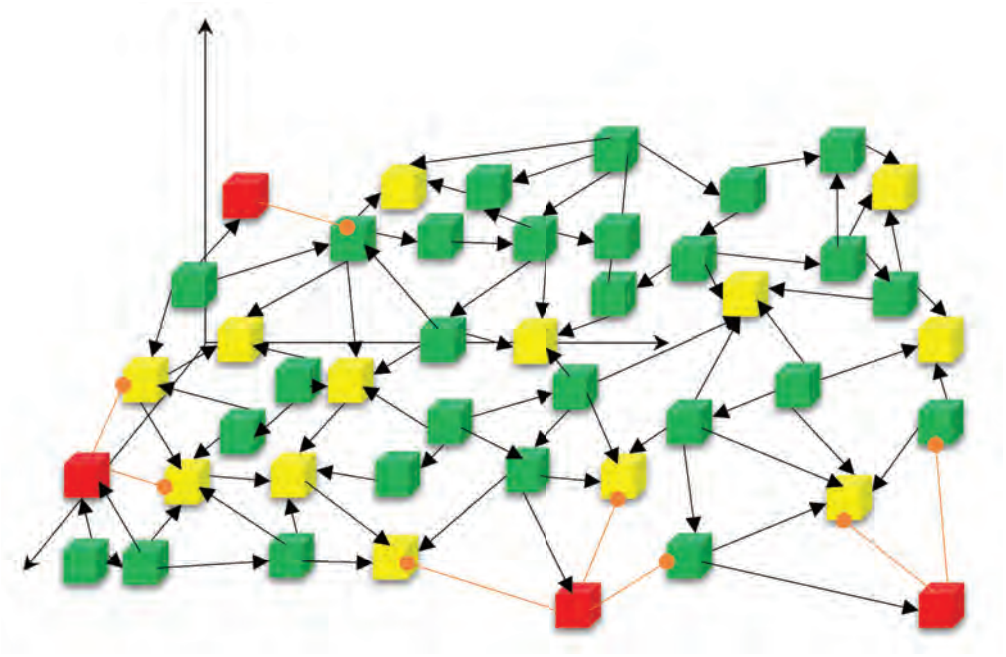

Рис. 5. Пример формирования поля решений деструктора

Вывод перед заключением: особенностью разработанной модели бот-сети интеллектуального деструктора является свойство адаптивности, основанное на полиморфной модели вирусных атак и метаморфной модели построения сценариев последовательных атак. Разработанный механизм позволяет визуализировать деятельность бот-сети в оперативном режиме.

Заключение

Данная статья является очередным звеном цикла статей по организации контура безопасности систем защиты информации корпоративных сетей любого уровня. Ранее были рассмотрены и подробно расшифрованы моменты, связанные с формализацией процессов современных систем деструкторов. Первый подготовительный этап в статье не рассматривается, так как достаточно подробно на примерах разбирается другими авторами в ведущих журналах (в статье приведено несколько ссылок с примерами). Используемые механизмы мультимножеств процессных моделей также рассматривались в многих публикациях, в данной статье приведено только разработанное решение при использовании заложенных ранее теоретических основах.

Приведенный пример поля решений использовался при проектировании контура безопасности в организации, охватывающей систему документооборота филиальной сети нескольких субъектов РФ. Используемые программные продукты (*KAV*, *Dallas*, *ViP Net* и др.) для организации защищенных сегментов подключены к единой системе мониторинга, так как кроссплатформенные системы позволяют подключать файлы отчетов к внешним системам. Прописанный код и результаты мониторинга за выделенный период по атакам и защитам будут представлены в последующих публикациях.

Литература

1. Ryzhenko A. A. Model of facet and hierarchical pyramidal system of support of management of information space of corporation. System analysis in economics – 2018: Proceedings of the V International research and practice conference-biennale (21-23 november 2018). – Moscow, Prometheus publishing house, 2018. – pp. 146-149.
2. Рыженко А. А. Формирование центров адаптации ресурсов как необходимого элемента международного сотрудничества / Большая Евразия: развитие, безопасность, сотрудничество. Ежегодник. – М.: ИНИОН РАН, 2018. – Вып.1, ч.1. – С. 327-328.
3. Julien Duchêne, Colas Le Guernic, Eric Alata, Vincent Nicomette & Mohamed Kaâniche State of the art of network protocol reverse engineering tools. Journal of Computer Virology and Hacking Techniques volume 14, pages53-68 (2018)
4. Razieh Eskandari, Mahdi Shajari & Mojtaba Mostafavi Ghahfarokhi ERES: an extended regular expression signature for polymorphic worm detection. Journal of Computer Virology and Hacking Techniques volume 15, pages177–194 (2019)
5. Hadis Ghanei, Farnoush Manavi & Ali Hamzeh, A novel method for malware detection based on hardware events using deep neural networks. Journal of Computer Virology and Hacking Techniques, volume 17, pages 319-331 (2021)

6. Varshini Reddy, Naimisha Kolli & N. Balakrishnan, Malware detection and classification using community detection and social network analysis. Journal of Computer Virology and Hacking Techniques, volume 17, pages 333-346 (2021)
7. Samanvitha Basole, Fabio Di Troia & Mark Stamp Multifamily malware models. Journal of Computer Virology and Hacking Techniques volume 16, pages79-92 (2020)
8. Mina Ebrahim & Seyed Alireza Hashemi Golpayegani, Anomaly detection in business processes logs using social network analysis. Journal of Computer Virology and Hacking Techniques, volume 18, pages 127-139 (2022)
9. Francesco Mercaldo & Antonella Santone, Audio signal processing for Android malware detection and family identification. Journal of Computer Virology and Hacking Techniques, volume 17, pages 139-152 (2021)
10. Рыженко А. А. Пирамидальная модель распределения информационных ресурсов госкорпораций на фасетно-иерархическом уровневом основании / А.А. Рыженко, Н.Ю. Рыженко // Анализ, моделирование, управление, развитие социально-экономических систем: сборник научных трудов XIII Всероссийской с международным участием школы-симпозиума АМУР-2019, Симферополь-Судак, 14-27 сентября 2019 / ред. совет: А.В. Сигал (предс.) и др. – Симферополь : ИП Корниенко А.А., 2019. – с. 346-353 ISBN 978-5-6042038-4-2
11. Рыженко А. А. Модифицированный алгоритм вируса полиморфика как основа деструктора информационной среды / Информатика: проблемы, методология, технологии: сборник материалов XVIII международной научно-методической конференции: в 7 т. / под редакцией Н.А. Тюкачева; Воронеж, Воронежский государственный университет, 14-15 февраля 2019 г. – Воронеж: Издательство «Научно-исследовательские публикации» (ООО «Вэлборн»), 2019. – Т. 5. – С. 857–861.
12. Jiaxing Cheng, Ying Li, Cheng Huang, Ailing Yu & Tao Zhang ACER: detecting Shadowsocks server based on active probe technology. Journal of Computer Virology and Hacking Techniques volume 16, pages217–227 (2020)
13. Рыженко А. А. Модель деструктора-полиморфа цифровой среды / Проблемы управления безопасностью сложных систем: материалы XXVI Междунар. конфер., 19 декабря 2018 г., Москва / под общ. ред. А. О. Калашникова, В.В. Кульбы. М.: ИПУ РАН, 2018. – с. 158–162.
14. Rizwan Ur Rahman & Deepak Singh Tomar, Threats of price scraping on e-commerce websites: attack model and its detection using neural network. Journal of Computer Virology and Hacking Techniques, volume 17, pages 75-89 (2021)
15. Рыженко А. А. Безопасность информации цифровой экономики / А. А. Рыженко, Н. Ю. Рыженко // Актуальные проблемы и перспективы развития экономики. Труды Юбилейной XX Всероссийской с международным участием научно-практической конференции. Симферополь, 2021. С. 289–291.
16. Systems of Systems Characterization and Types - NATO STO. URL: https://www.sto.nato.int/publications/STO%20Educational%20Notes/STO-EN-SCI-276/EN-SCI-276-01.pdf (дата обращения: 15.08.2023)

SMART BOTNET OR INTELLIGENT DESTRUCTOR MODEL

***Ryzhenko A.A.*[5]**

The aim of the work *is to develop a model of an intelligent botnet destructor containing autonomous and semi-autonomous resources.*

Research method: *multiset methods, conceptual modeling, process algorithmizing.*

Research result: *a model for the formation of rules for the transition of states of intelligent destructors of a single network as an autonomous element and as part of a single network at the same time has been developed. A feature of the model is its adaptability to external disturbances using an agent-based model of the methodology of a system of systems and the semantics of connections between them using a single indestructible core of the rule base and multiple choice of the tree-like hierarchy of the decision field of association bases. Production-type rules are presented in a simplified algebraic form by analogy with modern algorithms for constructing a digital signature (organization of a trust zone with public keys). The resulting statement solves such a problem as the natural appearance of hermits and outcasts in the form of single-tasking autonomous, which was one of the key problems of polymorphic destructors.*

The scientific novelty *lies in the development of a new element of conceptual modeling of model destructors - an attributive process that allows you to adaptively change the rules for the transition of states.*

Keywords: *destructor, modeling, intelligent agent, facet, hierarchy, transition rules, autonomous, decision field, polymorphic.*

5 Aleksey A. Ryzhenko, Ph.D., Associate Professor, Financial University under the Government of the Russian Federation, Moscow, AARyzhenko@fa.ru

References

1. Ryzhenko A.A. Model of facet and hierarchical pyramidal system of support of management of information space of corporation. System analysis in economics – 2018: Proceedings of the V International research and practice conference-biennale (21-23 november 2018). – Moscow, Prometheus publishing house, 2018. – pp. 146-149.
2. Ryzhenko A.A. Formirovanie centrov adaptacii resursov kak neobhodimogo jelementa mezhdunarodnogo sotrudnichestva / Bol'shaja Evrazija: razvitie, bezopasnost', sotrudnichestvo. Ezhegodnik. – M.: INION RAN, 2018. – Vyp.1, ch.1. – S. 327-328.
3. Julien Duchêne, Colas Le Guernic, Eric Alata, Vincent Nicomette & Mohamed Kaâniche State of the art of network protocol reverse engineering tools. Journal of Computer Virology and Hacking Techniques volume 14, pages53-68 (2018)
4. Razieh Eskandari, Mahdi Shajari & Mojtaba Mostafavi Ghahfarokhi ERES: an extended regular expression signature for polymorphic worm detection. Journal of Computer Virology and Hacking Techniques volume 15, pages177–194 (2019)
5. Hadis Ghanei, Farnoush Manavi & Ali Hamzeh, A novel method for malware detection based on hardware events using deep neural networks. Journal of Computer Virology and Hacking Techniques, volume 17, pages 319-331 (2021)
6. Varshini Reddy, Naimisha Kolli & N. Balakrishnan, Malware detection and classification using community detection and social network analysis. Journal of Computer Virology and Hacking Techniques, volume 17, pages 333-346 (2021)
7. Samanvitha Basole, Fabio Di Troia & Mark Stamp Multifamily malware models. Journal of Computer Virology and Hacking Techniques volume 16, pages79-92 (2020)
8. Mina Ebrahim & Seyed Alireza Hashemi Golpayegani, Anomaly detection in business processes logs using social network analysis. Journal of Computer Virology and Hacking Techniques, volume 18, pages 127-139 (2022)
9. Francesco Mercaldo & Antonella Santone, Audio signal processing for Android malware detection and family identification. Journal of Computer Virology and Hacking Techniques, volume 17, pages 139-152 (2021)
10. Ryzhenko A.A. Piramidal'naja model' raspredelenija informacionnyh resursov goskorporacij na fasetno-ierarhicheskom urovnevom osnovanii / A.A. Ryzhenko, N.Ju. Ryzhenko // Analiz, modelirovanie, upravlenie, razvitie social'no-jekonomicheskih sistem: sbornik nauchnyh trudov XIII Vserossijskoj s mezhdunarodnym uchastiem shkoly-simpoziuma AMUR-2019, Simferopol'-Sudak, 14-27 sentjabrja 2019 / red. sovet: A.V. Sigal (preds.) i dr. – Simferopol' : IP Kornienko A.A., 2019. – s. 346-353 ISBN 978-5-6042038-4-2
11. Ryzhenko A.A. Modificirovannyj algoritm virusa polimorfika kak osnova destruktora informacionnoj sredy / Informatika: problemy, metodologija, tehnologii: sbornik materialov XVIII mezhdunarodnoj nauchno-metodicheskoj konferencii: v 7 t. / pod redakciej N.A. Tjukacheva; Voronezh, Voronezhskij gosudarstvennyj universitet, 14-15 fevralja 2019 g. – Voronezh: Izdatel'stvo «Nauchno-issledovatel'skie publikacii» (OOO «Vjelborn»), 2019. – T. 5. – S. 857-861.
12. Jiaxing Cheng, Ying Li, Cheng Huang, Ailing Yu & Tao Zhang ACER: detecting Shadowsocks server based on active probe technology. Journal of Computer Virology and Hacking Techniques volume 16, pages217–227 (2020)
13. Ryzhenko A.A. Model' destruktora-polimorfa cifrovoj sredy / Problemy upravlenija bezopasnost'ju slozhnyh sistem: materialy HHVI Mezhdunar. konfer., 19 dekabrja 2018 g., Moskva / pod obshh. red. A.O. Kalashnikova, V.V. Kul'by. M.: IPU RAN, 2018. – s. 158-162.
14. Rizwan Ur Rahman & Deepak Singh Tomar, Threats of price scraping on e-commerce websites: attack model and its detection using neural network. Journal of Computer Virology and Hacking Techniques, volume 17, pages 75-89 (2021)
15. Ryzhenko A.A. Bezopasnost' informacii cifrovoj jekonomiki / A.A. Ryzhenko, N.Ju. Ryzhenko // Aktual'nye problemy i perspektivy razvitija jekonomiki. Trudy Jubilejnoj XX Vserossijskoj s mezhdunarodnym uchastiem nauchno-prakticheskoj konferencii. Simferopol', 2021. S. 289-291.
16. Systems of Systems Characterization and Types - NATO STO. URL: https://www.sto.nato.int/publications/STO%20Educational%20Notes/STO-EN-SCI-276/EN-SCI-276-01.pdf (data obrashhenija: 15.08.2023)