УДК 004.056.53

Е.А. Басыня, В.Е. Хиценко, А.А. Рудковский

Метод идентификации киберпреступников, использующих инструменты сетевого анализа информационных систем с применением технологий анонимизации

Представлен анализ современных подходов хакеров к проведению кибератак, подробно описана одна из стратегий исследования объекта атаки с использованием комбинирования виртуальных защищенных каналов связи, средств анонимизации, включая оверлейные технологии и сети. Предложен оригинальный метод противодействия подобным несанкционированным воздействиям. Научная новизна работы заключается в идентификации злоумышленников (осуществляющих активный сбор данных с применением технологий анонимизации) посредством составления векторов атаки на основе ряда параметров: принадлежности адресного пространства к сети анонимизации, исчерпания пула адресного пространства (личностей) сети анонимизации, типа активного/пассивного исследования, хода выполнения типа исследования, корреляции параметров с привносимыми искусственными задержками и др. Выносимый на обзор метод идентификации злоумышленников, использующих инструменты автоматизированного активного и пассивного анализа трафика и информационных систем с применением технологий анонимизации, используется совместно с авторским модулем фальсификации операционных систем и функционирующих на них сервисов/служб в широком спектре вариаций для различных хакеров, что позволяет успешно дезинформировать злоумышленника на первом этапе проведения кибератаки. Программная реализация авторского метода была успешно протестирована, экспериментально исследована и апробирована. Целевой областью применения выступают серверные решения, функционирующие на основе стека протоколов TCP/IP.

Ключевые слова: анонимизация, оверлейные сети, сканирование, зондирование, дезинформация.
doi: 10.21293/1818-0442-2019-22-2-45-51

Автоматизация информационных процессов всех сфер общественной деятельности не только выступает катализатором их развития, но и порождает широкий спектр уязвимостей, которые могут быть использованы для проведения кибератак. Лишь на критическую информационную инфраструктуру Российской Федерации в прошлом году было совершено более 4,3 миллиарда кибератак согласно данным Национального координационного центра по компьютерным инцидентам [1]. Последствия успешного взлома информационной системы и сети проявляются в существенных экономических и политических издержках. В качестве примера стоит привести кражу биткоинов на $120 млн у криптовалютной биржи Youbit, кражу конфиденциальных данных (от идентификаторов социального страхования до номеров кредитных карт) 145 млн клиентов крупного кредитного агентства Equifax [2].

Проблематика информационной безопасности заключается в несовершенстве стека протоколов TCP/IP и уязвимостях программного обеспечения (ПО): от операционных систем до прикладных утилит. С течением времени быстро нарастает актуальность обеспечения сетевой информационной безопасности.

Для достижения этой цели телекоммуникационными компаниями и научным сообществом разрабатываются различные программные и аппаратно-программные решения. Стоит отметить, что одновременно и киберпреступники совершенствуют свой инструментарий и методики: от этапа первичного сбора информации об объекте исследования до его успешного взлома или вывода из состояния доступности. Данное противостояние не имеет устойчивого баланса.

Для ограничения и блокировки сбора информации о системе со стороны неавторизованного объекта разрабатываются различные методы противодействия сетевому сканированию: от реализации скрытых каналов исследования до использования подхода к идентификации аномалий [3–5]. Но данные методы не дают однозначного результата в случае применения киберпреступником комбинирования оверлейных технологий и различных средств анонимизации.

В данной работе будут проанализированы современные подходы хакеров к пассивному и активному анализу информационных систем и сетей, а также предложен оригинальный метод противодействия внешним злоумышленным возмущениям.

Постановка задачи

Целью данной работы являлись разработка, исследование и программная реализация метода идентификации злоумышленников, использующих инструменты автоматизированного активного и пассивного анализа трафика и информационных систем в последовательном режиме с применением технологий анонимизации. Данный метод используется в авторском модуле фальсификации операционных систем и функционирующих на них сервисов/служб в широком спектре вариаций для различных хакеров [6, 7]. Определенный сфальсифицированый снимок программного обеспечения предоставляется конкретному идентифицированному хакеру, несмотря на его попытки анонимизации. Полноценное дезинформирование хакера выступает качественным ин-

струментом защиты и позволяет отследить дальнейшие (ответные) действия злоумышленника.

Анализ существующих стратегий проведения кибератак

С целью извлечения экономической и политической выгоды преступное сообщество прибегает к несанкционированному доступу к информационным ресурсам, организует взлом и вывод объектов из состояния доступности. Для решения поставленных задач разрабатываются различные стратегии проведения кибератак. Одним из первых и ключевых этапов любого плана злоумышленника выступает сбор информации о целевой системе или сети как в техническом, так и в организационном аспекте. Фактически разведка позволяет определить топологию и структуру вычислительной сети, используемые аппаратно-программные решения, их архитектуру и уязвимости. На данном этапе применяются механизмы пассивного и активного анализа трафика и информационных ресурсов.

Этот этап представляет собой пассивную аккумуляцию информации и рекогносцировку с целью получения данных, относящихся к целевым объектам, без непосредственного участия самих объектов. Примером таких инструментов являются снифферы (перехватчики и сетевые анализаторы трафика), а также системы OSINT (англ. open source intelligence – разведка на основе открытых источников) [8].

Активный метод предполагает взаимодействие с целевой системой во время сбора информации. На этой основе функционируют инструменты сканирования, пентестинга (тестирование на проникновение) и зондирования. При сканировании исследуют открытые TCP- и UDP-порты, определяют функционирующие на ней сервисы и службы, распознают тип операционной системы. Пентестинг используется для оценки безопасности систем путем имитации атаки. В ходе зондирования имитируются различные атаки и отслеживается реакция объекта с идентификацией эшелонов его защиты и формируются рекомендации по взлому защиты.

Наиболее распространенный элемент стратегии проведения кибератак – сканирование портов [9]. Существующие системы обнаружения и предотвращения вторжений легко блокируют подобные внешние возмущения, если с одного IP-адреса производится подключение к двум и более портам. С данной задачей справляются даже антивирусные средства.

Более эффективным методом несанкционированного исследования информационных систем является вертикальное распределенное сканирование [10], позволяющее задействовать множество IP-адресов для сканирования большого диапазона портов на одной целевой системе. Этот метод позволяет злоумышленнику минимизировать вероятность его обнаружения, а также исключает возможности существующих средств защиты для блокировки атакующего.

Не все угрозы, исходящие от злоумышленников, можно считать одинаково опасными. Некоторые из них являются просто малозначительными неприятностями, другие потенциально угрожают развитию и существованию организации. В наиболее разрушительных угрозах можно выделить три важных показателя:

- скорость исполнения;
- интенсивность;
- неожиданность.

Скорость и интенсивность – это технические преимущества, для которых можно найти ответные решения. Если сетевая инфраструктура предприятия имеет комплексный контроль информационной безопасности, то возможно отразить быстрые и агрессивные атаки. Однако в случае постобработки или привнесения задержек системами защиты атака может достичь цели. При этом важно однозначно идентифицировать злоумышленника даже при сканировании защищенных систем [11, 12].

Совокупность применяемых алгоритмов и методов несанкционированного исследования и взлома информационных систем в сочетании с используемыми программными решениями позволяет ввести следующую классификацию злоумышленников по уровню квалификации:

- начального уровня;
- среднего уровня;
- высокого уровня.

Злоумышленники начального уровня не имеют практического опыта, атакуют с одного IP-адреса, своевременно идентифицируются и блокируются современными средствами обеспечения безопасности: системами обнаружения и предотвращения вторжения, межсетевыми экранами и антивирусными программами. При проведении подобных атак используется программное обеспечение, которое представлено в свободном доступе, присутствует во всех базах знаний систем защиты, как и эксплуатируемые известные уязвимости. Таких злоумышленников легко деанонимизировать, так как они прикладывают минимум усилий для сокрытия своей локации.

Злоумышленники среднего уровня квалификации задействуют расширенные методы сканирования портов: от низкозатратного по производительности сканирования SYN-пакетами до сессионного взаимодействия прикладными протоколами. В дополнение атакующие используют проксисерверы и технологии виртуальных защищенных каналов связи (например, VPN – англ. virtual private network) для обхода систем защиты и сокрытия своего реального месторасположения. Деанонимизация подобных хакеров также не составляет труда для глобального наблюдателя, способного на уровне интернет-провайдера производить описанное ниже исследование связи параметров информационных потоков на основе привнесения задержек.

Злоумышленники высокого уровня квалификации формируют стратегию проведения кибератак с использованием комбинирования виртуальных защищенных каналов связи, средств анонимизации,

оверлейных технологий и сетей. Под оверлейной сетью (англ. Overlay Network) в данном контексте понимается общий случай логической сети, создаваемой поверх Интернета, функционирующего на основе стека протоколов TCP/IP. Узлы оверлейной сети могут быть связаны физическим или логическим соединением, для которого в основной сети существует один или несколько соответствующих маршрутов из физических соединений.

Описанная стратегия проведения кибератаки, позволяющая обойти существующие системы защиты и обеспечить анонимность хакера, представлена на рис. 1.

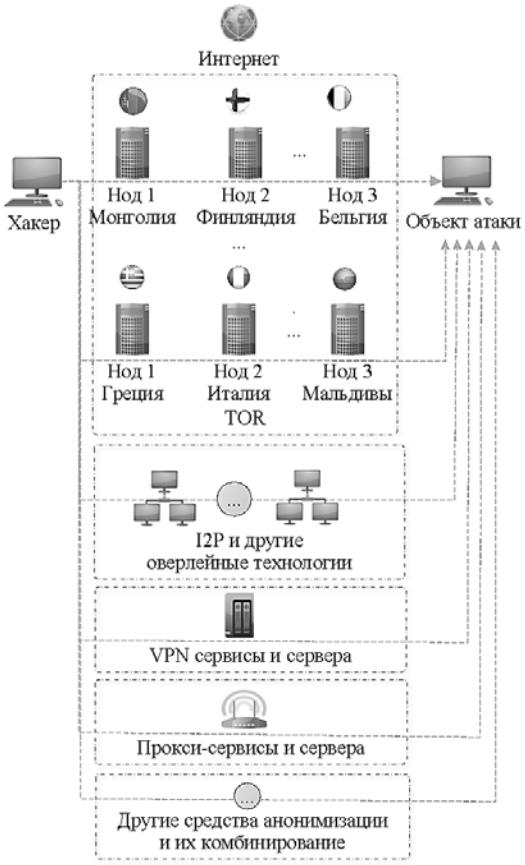

Рис. 1. Стратегия проведения кибератаки

В основе представленной стратегии лежит комбинирование виртуальных защищенных каналов связи, средств анонимизации, оверлейных технологий и сетей. На первом этапе злоумышленник выбирает последовательность использования перечисленных технологий и разворачивает соответствующую программную инфраструктуру. Далее в рамках активного воздействия на объект атаки злоумышленник организует любое атомарное информационное взаимодействие с одного IP-адреса. По окончании данной итерации меняется личность (IP-адрес и сеть в случае исчерпания ресурсов). Данные действия повторяются до окончания несанкционированного исследования информационной системы.

В качестве примера стоит привести последовательность действий при сканировании TCP- и UDP-портов операционной системы жертвы:

1) составление последовательности используемых технологий: TOR, I2P+Mixminion, VPN-сервисы, проксисервисы;

2) развертка программной инфраструктуры стека технологий из первого пункта;

3) построение цепочки оверлейной сети TOR;

4) сканирование одного порта с одной выходной ноды сети TOR;

5) перестроение цепочки оверлейной сети TOR;

6) сканирование одного порта с новой выходной ноды сети TOR;

7) повторение п. 3–6 до исчерпания IP-адресов выходных нод сети TOR;

8) смена пула адресного пространства на сети I2P+Mixminion и повторение действий, аналогичных п. 3–7;

9) смена пула адресного пространства на сервисы VPN и повторение действий, аналогичных п. 3–7.

10) смена пула адресного пространства на прокси-сервисы и повторение действий, аналогичных п. 3–7;

11) составление отчета о результатах сканирования.

Таким образом, успешно осуществляется анонимное сканирование TCP- и UDP-портов операционной системы жертвы. Подобная комплексная стратегия проведения кибератаки является нетривиальной и ресурсозатратной, а также требует высокого уровня квалификации злоумышленника. Предлагаемый авторами метод идентификации киберпреступников, использующих инструменты сетевого анализа информационных систем с применением технологий анонимизации, может быть применен в качестве механизма защиты от атак подобного рода.

Проблематика атакующей стороны

В настоящее время злоумышленнику достаточно проблематично организовать масштабное сканирование самостоятельно, так как для аренды большого числа серверов требуются серьезные финансовые вложения. Вдобавок к этому необходима верификация пользователя, что еще больше мешает преступнику осуществить свои намерения.

Так, популярные дата-центры и провайдеры при первичном запросе услуги могут потребовать подтверждение личности. Требуются документы, на основании которых можно без затруднений идентифицировать клиента. Интересной практикой является необходимость предоставления фото человека с определенным документом в руках, что позволяет убедиться в подлинности личности субъекта.

С технической точки зрения злоумышленнику осложняют деятельность публичные базы знаний IP-адресов различных сервисов анонимизации, запросы с которых могут отклоняться средствами защиты жертвы по политике DROP (без уведомлений).

К сожалению, любые ограничения могут быть нейтрализованы хакером высокого уровня квалификации.

Проблематика стороны защиты

Стек протоколов TCP/IP изначально не был спроектирован с учетом высоких требований к ин-

формационной безопасности [13]. Даже базовые протоколы и алгоритмы не предусматривают проверки подлинности субъектов взаимодействия.

Несовершенство программного обеспечения позволяет атакующей стороне использовать различные уязвимости системы для проведения атаки.

Другим немаловажным моментом выступает отсутствие единой актуальной базы знаний «подозрительных» IP-адресов. К тому же в силу свободы слова не стоит исключать возможность доступа с этих адресов добропорядочных пользователей.

Принятая жесткая логика поведения средств защиты не только упрощает идентификацию злоумышленником средств защиты жертвы, но и зачастую плохо выстроена. Например, большинство систем обнаружения и предотвращения вторжений начинают сигнализировать о подозрительной сетевой активности лишь при исследовании более двух нестандартных портов с одного IP-адреса.

Технические ограничения существующих систем защиты учитываются злоумышленником при проектировании стратегии атаки. Например, большинство межсетевых экранов для блокировки запросов с различных анонимных сетей ведут черный список, размещенный в пакетном фильтре IPTABLES [14], что замедляет работу системы. Это связано с последовательной обработкой записей от первого правила к последнему. При этом есть ограничения как на количество источников в одном правиле, так и на общее количество правил. Соответственно исключается полноценное противостояние ранее описанной комплексной стратегии проведения профессиональной кибератаки.

Предлагаемое решение

В данной работе предложен оригинальный метод идентификации злоумышленников, использующих инструменты автоматизированного активного и пассивного анализа трафика и информационных систем в последовательном режиме с применением технологий анонимизации (рис. 2).

Рассмотрим работу системы, функционирующей на основе данного метода. Программная часть была спроектирована и реализована с использованием следующего стека технологий: операционная система Alpine Linux, языки программирования Python, C++, фреймворк Flask, СУБД PostgreSQL, системы управления репозиториями и проектами GitLab и Redmine, системы управления виртуальной инфраструктурой разработки: ESXI, Docker, Vagrant, модули оверлейных сетей и др.

На первом этапе работы метода производится синхронизация с публичными списками сетей анонимизации: прокси- и VPN-сервисов.

Далее процесс синхронизации переключается на публичные черные списки IP-адресов [15], причинами внесения в которые являются спам, ботнет, DDOS и иные атаки.

Затем заранее установленное программное обеспечение для доступа к оверлейным технологиям и сетям позволяет, используя внутренние инструменты/интерфейсы, запросить актуальный список IP-адресов всех выходных нодов.

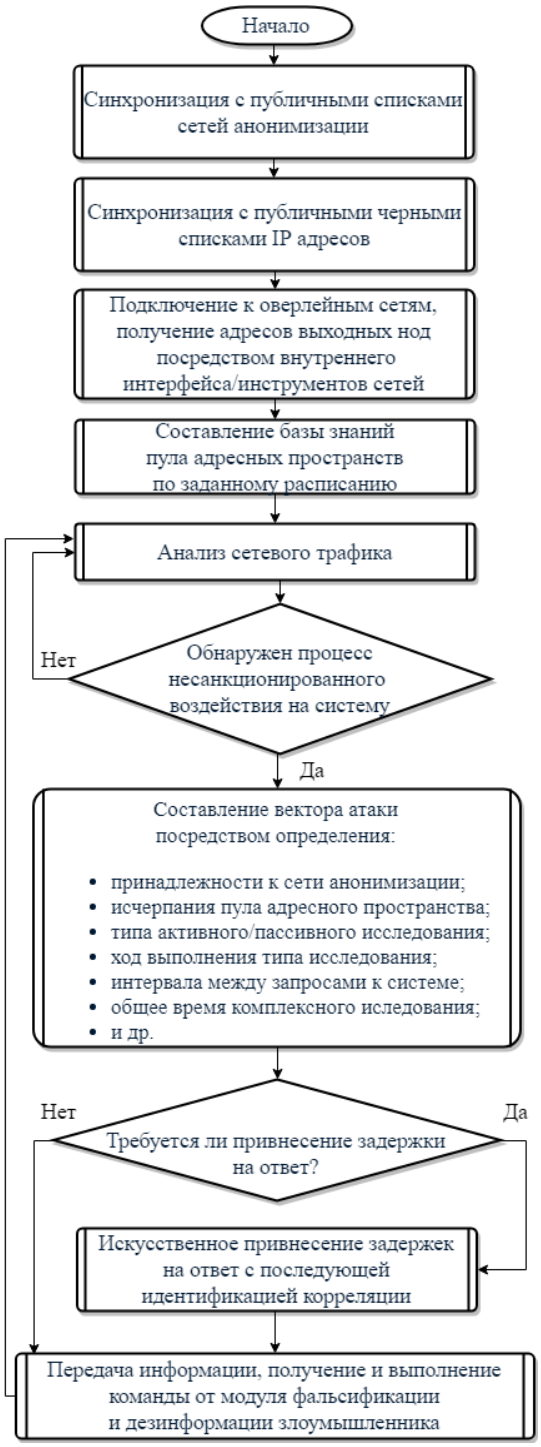

Рис. 2. Блок-схема предлагаемого метода

В результате выполнения описанных действий производится итерационное составление базы знаний пула адресных пространств. Период обновления базы знаний можно устанавливать вручную. Значение по умолчанию – 1 ч. Все базы данных обслуживает локальная система управления базами данных.

С целью идентификации определенного злоумышленника из группы атакующих в онлайн режиме производится мониторинг и анализ сетевого

трафика для выявления информационных потоков по следующим признакам:

- принадлежность адресного пространства к сети анонимизации;
- регистрация исчерпания пула адресного пространства (личностей) сети анонимизации;
- тип активного/пассивного исследования;
- регистрация хода выполнения типа исследования;
- интервал между запросами к системе;
- и др.

Совокупность этих признаков формирует вектор атаки, который позволяет определить хакера за множеством сменяемых личностей.

Для повышения вероятности сопоставления вектора атаки конкретному злоумышленнику используется искусственное привнесение задержек на ответ с последующей идентификацией корреляции.

Стоит отметить, что данный метод используется в авторском модуле фальсификации определенной конфигурации программного обеспечения (операционной системы и функционирующих на ней сервисов/служб) с ориентацией на конкретного хакера, несмотря на использование им технологий анонимизации. Соответственно одним из последних этапов предлагаемого метода является передача информации, получение и выполнение команды от модуля фальсификации и дезинформации злоумышленника.

Обнаружение несанкционированного исследования системы производится стандартными сигнатурными методами. Например, обращение к любому порту, не предоставляющему публичный сервис клиентам, можно считать потенциальным вредоносным возмущением.

В рамках поставленной задачи был сделан акцент на последовательную методику исследования сети/системы злоумышленником. Это связано с анализом накопленной статистики по проводимым комплексным атакам злоумышленниками с использованием и комбинированием средств анонимизации. Большинство автоматизированных средств исследования при перенаправлении трафика через оверлейные сети конфигурируются в рамках последовательной стратегии «итерация исследования – ожидание ответа – смена личности». Это может быть связано как с техническими ограничениями сети, так и со сложностью и ресурсоемкостью организации параллельного сканирования. Для такого сканирования используются другие признаки вектора атаки, при этом вероятность идентификации хакера снижается. В случае невозможности идентификации система может просто фальсифицировать определенный снимок программного обеспечения при сканировании из одной сети в определенный кратко- и среднесрочный интервал времени.

При комплексном примитивном сканировании с одного IP-адреса система фиксирует низкий уровень опасности и предоставляет идентичный слепок ПО для всех типов сканирования/зондирования.

В функционал системы была также заложена функция блокировки доступа к различным пулам адресных пространств. На стадии проектирования системы была внедрена нулевая маршрутизация. Blackhole – в UNIX-системах маршрутизация «в никуда». Необходимые информационные потоки отбрасываются в силу отсутствия маршрута до хоста. Данным подходом был нейтрализован существенный недостаток существующих решений защиты: критичное замедление работы при большом объеме правил и адресов в пакетном фильтре с общим ограничением на их количество.

Обсуждение результатов и заключение

В данной работе были проанализированы современные подходы хакеров к проведению кибератак, описана одна из стратегий с использованием комбинирования виртуальных защищенных каналов связи, средств анонимизации, оверлейных технологий и сетей. Предложен оригинальный подход к противодействию подобным несанкционированным воздействиям.

Научная новизна заключается в идентификации злоумышленников (осуществляющих активный сбор данных с применением технологий анонимизации) посредством составления векторов атаки на основе ряда признаков: принадлежность адресного пространства к сети анонимизации, исчерпание пула адресного пространства (личностей) сети анонимизации, тип активного / пассивного исследования, ход выполнения типа исследования, корреляция с искусственными задержками и др.

Программная реализация данного проекта была успешно протестирована в ручном и автоматизированном режимах. Данный метод используется в авторском модуле фальсификации функционирующего программного обеспечения на объекте исследования для различных хакеров. Для проведения экспериментальной проверки метода 50 специалистов в сфере информационной безопасности анонимно исследовали модельный объект в течение недели и представили список идентифицированных ОС, сервисов и служб. Сводный протокол результатов продемонстрировал успешность метода в 96% случаев. 4% неудачной защиты относятся к 8 участникам эксперимента, которые применяли параллельное сканирование в единый момент времени из пула одной сети анонимизации. При этом система не выдала себя несопоставимыми ответами, действия в состоянии неопределенности сводились к имитации закрытого порта либо выдачи идентичной информации нескольким источникам с тождественным «слепком» объекта. Важно понимать, что принципиально невозможно обеспечить гарантированный уровень безопасности информационных ресурсов.

Достигнутые результаты в полном объеме удовлетворяют требованиям поставленной задачи. С практической точки зрения данные решения могут быть использованы в межсетевых экранах и шлюзах вычислительных сетей.

Литература

1. За год на Россию было совершено более четырех миллиардов кибератак [Электронный ресурс]. – Режим доступа: https://rg.ru/2018/12/12/za-god-na-rossiiu-bylo-

soversheno-bolee-chetyreh-milliardov-kiberatak.html, свободный (дата обращения: 2019.03.22)

2. Отчет по информационной безопасности [Электронный ресурс]. – Режим доступа: http://rrc.ru/upload/checkpoint/analytic_reports/check%20point_25052018_Screen_Letter_RUSv3bis.pdf, свободный (дата обращения: 2019.03.22).

3. Способы противодействия сетевому сканированию / А.В. Болдырев, Д.Ю. Верещагин, А.Г. Жулькин, А.Б. Рагудеев // Информационная безопасность. – 2016. – № 3, т. 1. – С. 401–404.

4. Implementation and vulnerability test of stealth port scanning attacks using ZMap of censys engine. / S. Lee, S. Im, S. Shin, B. Roh, C. Lee // International Conference on Information and Communication Technology Convergence (ICTC). – Jeju. – 2016. – P. 681–683.

5. Ananin E.V. Port scanning detection based on anomalies / E.V. Ananin, A.V. Nikishova, I.S. Kozhevnikova // Dynamics of Systems, Mechanisms and Machines (Dynamics). – Omsk, 2017. – P. 1–5.

6. Французова Г.А. Самоорганизующаяся система управления трафиком вычислительной сети: метод противодействия сетевым угрозам / Г.А. Французова, А.В. Гунько, Е.А. Басыня // Программная инженерия. – 2014. – № 3. – С. 16–20.

7. Басыня Е.А. Самоорганизующаяся система управления трафиком вычислительной сети / Е.А. Басыня, Г.А. Французова, А.В. Гунько // Доклады ТУСУР. – 2014. – № 1 (31). – С. 179–184.

8. Open-source intelligence [Электронный ресурс]. – Режим доступа: https://en.wikipedia.org/wiki/Open-source_intelligence, свободный (дата обращения: 2019.03.24).

9. Кожевникова И.С. Исследование методов обнаружения сканирования портов / И.С. Кожевникова, А.О. Пасюк // Вестник ВолГУ. Сер. 9: Исследования молодых ученых. – 2016. – № 14. – С. 30–31.

10. Анализ атак с использованием сканирования портов [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/analytics/Threats_Analysis/Examining-Port-Scan-Attacks, свободный (дата обращения: 2019.03.24).

11. Листеренко Р.Р. Продвинутые атаки требуют новых видов защиты информации / Р.Р. Листеренко, В.Г. Карабатырова // Вопросы кибербезопасности. – 2013. – № 2. – С. 34–39.

12. Лазаренко А.В. Технологии деанонимизации пользователей Tor // Новые информационные технологии в автоматизированных системах. – 2016. – №19. – С. 257–262.

13. Бойченко О.В. Модель osi в защите данных корпоративной сети / О.В. Бойченко, А.С. Ивченко // Инновационная наука. – 2016. – № 3-1 (15). – С. 114–116.

14. Чемодуров А.С. Защита интернет-шлюза и фильтрация сетевого трафика корпоративной сети / А.С. Чемодуров, А.Ю. Карпутина // Концепт. – 2015. – № 1. – С. 1–6.

15. Абдуллаев В.Г. Защита от спама в интернет-пространстве // Радиоэлектроника и информатика. – 2014. – № 2. – С. 35–38.

Басыня Евгений Александрович
Канд. техн. наук, доцент каф. автоматики
Новосибирского государственного технического университета (НГТУ),
директор Научно-исследовательского института информационно-коммуникационных технологий
Карла Маркса пр-т, д. 20, г. Новосибирск, Россия, 630073
ORCID 0000-0003-3916-7783
Тел: 8 (383-3) 46-11-19
Эл. почта: basinya@corp.nstu.ru

Хиценко Владимир Евгеньевич
Кандидат техн. наук, доцент
каф. защиты информации (ЗИ) НГТУ
Карла Маркса пр-т, д. 20, г. Новосибирск, Россия, 630073
Тел: +7 (383-3) 46-08-53
Эл. почта: xicenko@corp.nstu.ru

Рудковский Александр Александрович
Студент, каф. ЗИ НГТУ
Карла Маркса пр-т, д. 20, г. Новосибирск, Россия, 630073
ORCID 0000-0001-6856-3908
Тел: +7 (383-3) 46-08-53
Эл. почта: rudkovskiyalex@gmail.com

Basinya E.A., Khitsenko V.E., Rudkovskiy A.A.

Method to identify cybercriminals using network analysis of information systems with anonymization

In this paper, modern tactics of the hackers to conduct cyber-attacks were analyzed, a strategy to investigate an object of attack using the combined virtual secure communication channel, anonymization tools are described, including overlay technologies and networks. An original method of counteraction of such unauthorized activities is provided. The scientific novelty of the work consist in the identification of intruders (performing active harvest of the data using technology of anonymization) by making assault vectors based on a number of parameters. For example, address space belonging to anonymization network, pool exhaustion for anonymization network address space (identity), type of active/passive scan, progress of the scan type, correlation of the parameters due to artificial delays and etc. The method to identify the attackers who are using tools of the automated active and passive analysis of traffic and information systems by applying technologies of anonymization, described in the article, is used together with the author's module of falsification of operating systems and the services functioning on them in a wide range of variations for various hackers. This allows misinforming successfully hacker on first step of the cyber-attacks. The software implementation of the author's method was successfully tested, experimentally investigated. The target area of application are server solutions that operate based on the TCP/IP Protocol stack

Keywords: anonymization overlay networks, scanning, probing, misinformation.
doi: 10.21293/1818-0442-2019-22-2-45-51

References

1. Over a year, Russia has been committed more than four billion cyberattacks. Available at: https://rg.ru/2018/12/12/za-god-na-rossiiu-bylo-soversheno-bolee-chetyreh-milliardov-kiberatak.html (Accessed: March 22, 2019).

2. Information security report. Available at: http://rrc.ru/upload/checkpoint/analytic_reports/check%20point_25052018_Screen_Letter_RUSv3bis.pdf (Accessed: March 22, 2019)

3. Boldyrev A.V., Vereshchagin V., Zhulkin A.G., Yagudaev A.B. Sposoby protivodejstviya setevomu skanirovaniyu [Ways to counter network scannington]. *Information security*, 2016, no. 3, vol. 1, pp. 401–404.

4. Lee S., Im S., Shin S., Roh B., Lee C. Implementation and vulnerability test of stealth port scanning attacks using ZMap of censys engine. International Conference on Information and Communication Technology Convergence (ICTC), Jeju, 2016, pp. 681–683.

5. Ananin E.V., Nikishova A.V., Kozhevnikova I.S. Port scanning detection based on anomalies. *Dynamics of Systems, mechanics and Machines (Dynamics)*, Omsk, 2017, pp. 1–5.

6. Frantsuzova G.A., Gunko A.V., Basinya E.A. Samoorganizuyushchayasya sistema upravleniya trafikom vychislitel'noj seti: metod protivodejstviya setevym ugrozam [Self-organizing control system of computer network traffic: method to counter network threats]. *Software engineering*, 2014, no. 3, pp. 16–20.

7. Basinya E.A., Frantsuzova G.A., Gunko A.V. Samoorganizuyushchayasya sistema upravleniya trafikom vychislitel'noj seti [Self-organizing control system of computer network traffic]. *Proceedings of TUSUR University*, 2014, no. 1 (31), pp. 179–184.

8. Open-source intelligence. Available at: https://en.wikipedia.org/wiki/Open-source_intelligence (Accessed: March 24, 2019).

9. Kozhevnikova I.S., Pasyuk O.A. Issledovanie metodov obnaruzheniya skanirovaniya portov [The Study of methods of detecting port scanning]. *Bulletin of the Volga. Series 9: Research of young scientists*, 2016, no. 14, pp. 30–31.

10. Analysis of attacks using port scanning. Available at: https://www.anti-malware.ru/analytics/Threats_Analysis/Examining-Port-Scan-Attacks (Accessed: March 24, 2019).

11. Nesterenko R.R., Karabutov V.G. Prodvinutye ataki trebuyut novyh vidov zashchity informacii [Advanced attacks call for new kinds of information security]. *Cyber security issues*, 2013, no. 2, pp. 34–39.

12. Lazarenko V.A., Tekhnologii deanonimizacii pol'zovatelej Tor [Technology deanonimization Tor users]. *New information technologies in automated systems*, 2016, no. 19, pp. 257–262.

13. Boychenko O.V., Ivchenko A.S. *Model' osi v zashchite dannyh korporativnoj seti* [OSI Model in corporate network data protection]. *Innovative science*, 2016, no. 3-1 (15), pp. 114–116.

14. Chemodurov A.S., Carpatina A.Y. Zashchita internet-shlyuza i fil'traciya setevogo trafika korporativnoj seti [Protection of the Internet gateway and filtering network traffic corporate network]. *Considered*, 2015, no. 1, pp. 1–6.

15. Abdullayev V.G. Zashchita ot spama v Internet prostranstve [Protection against spam in the Internet space]. *Radioelectronics and Informatics*, 2014, no. 2, pp. 35–38.

Evgeny A. Basinya
Candidate of Engineering,
Assistant Professor, Automation Department
Novosibirsk State Technical University (NSTU)
20, Karl-Marks st., Novosibirsk, Russia, 630073
ORCHID 0000-0003-3916-7783
Phone: + 7 (383-3) 46-11-19
Email: basinya@corp.nstu.ru

Vladimir E. Khitsenko
Candidate of Engineering, Assistant Professor,
Protection of Information Department NSTU
20, Karl-Marks st., Novosibirsk, Russia, 630073
Phone: +7 (383-3) 46-08-53
Email: xicenko@corp.nstu.ru

Alexander A. Rudkovsky
Student, Protection of Information Department NSTU
20, Karl-Marks st., Novosibirsk, Russia, 630073
ORCHID 0000-0001-6856-3908
Phone: +7 (383-3) 46-08-53
Email: rudkovskiyalex@gmail.com