Инженерный вестник Дона, №11 (2024)
ivdon.ru/ru/magazine/archive/n11y2024/9651

Обзор технологий для обмана злоумышленника (ловушки, приманки, перемещение целей, платформа обмана), их классификация и взаимодействие

А.М. Тихонов

Финансовый университет при правительстве Российской Федерации

Аннотация: Цель статьи – произвести обзор различных видов обмана злоумышленников в сети, изучить применимость и вариативность современных технологий обмана. Метод изучения – анализ существующих статей в рецензируемых российских и зарубежных источниках, агрегация исследований, формирование выводов исходя из проанализированных источников. В обзорной статье рассматриваются технологии обмана злоумышленника (ловушки Honeypot, приманки Honeytoken, перемещение цели MTD, платформа обмана Deception). Указывается эффективность применения обмана с точки зрения воздействия на психическое состояние человека. В статье приводится описание различных видов ловушек, рассматривается классификация в зависимости от цели, места внедрения, уровня взаимодействия, расположения, типа внедрения, однородности и вида активности. а также их составляющие части. Рассматриваются различные стратегии применения ловушек в сети – жертвенный ягненок, хакерский зоопарк, минное поле, ловушки при сближении, экраны перенаправления, порты обмана. Приведена классификация приманок, описаны методы их применения в сети организации, указаны дополнительные условия, повышающие вероятность обнаружения злоумышленника с помощью приманки. Приведены основные методики стратегии MTD, позволяющие запутывать инфраструктуру. Описано взаимодействие этих техник с технологиями ловушек и приманок. Приводится исследование, которое подтверждает эффективность использования MTD вместе с ловушками и приманками, указаны сложности при использовании этой стратегии. Приведено описание Deception платформы, описаны её отличительные особенности от обычных ловушек и приманок, указана возможность её взаимодействия с MTD. В результате были выявлены и описаны основные технологии и стратегии обмана злоумышленника, указано их развитие, описано их противодействие злоумышленнику.

Ключевые слова: инфраструктура ложных целей, перемещение целей, ловушки, приманки, Deception Platform, Honeypot, Honeytoken, Honeynet, MTD, обман злоумышленника.

Введение

Одним из самых эффективных способов проникновения внутрь организации является фишинг атака, то есть атака, целью которой является обман сотрудника организации с целью получения несанкционированного доступа. Сотрудник компании выбирается в качестве наиболее легкодоступной цели с расчетом на его невнимательность и ошибку при

получении сообщения от злоумышленника. Согласно отчету Verizon с расследованием об утечке данных за 2019 год [1], фишинговые атаки составили более 80% зарегистрированных инцидентов безопасности от общего объема. Во время пандемии COVID19 мы стали свидетелями большого количества случаев, когда злоумышленники использовали общую взволнованность населения из-за коронавируса для проведения своих атак [2].

Обман направлен на манипулирование восприятием людей путем использования их психологической уязвимости. Благодаря воздействию на их восприятие, может быть оказано влияние на их убеждения, решения и действия [3]. Как раз это воздействие может стать эффективным инструментом в руках как злоумышленников, так и службы кибербезопасности. Еще в конце 1980-х Клиффорду Столлу удалось создать компьютерную среду (ныне известную как honeypot), в которой использовались фиктивная учетная запись и ложные документы с завлекающими злоумышленника названиями. Такая среда была призвана заставить злоумышленника провзаимодействовать с ней, тем самым раскрыв себя и свои цели [4]. В противостоянии между командой атаки и командой защиты, принято считать, что преимущество имеет команда атаки. Это связано с тем, что команде защиты необходимо следить за всей инфраструктурой организации, и предотвращать вторжения в каждой отдельной точке, в то время как злоумышленнику достаточно найти одну уязвимость, воспользовавшись которой он попадет во внутреннюю среду [5]. В дополнение к этому, злоумышленники всегда могут получить информацию о целевой системе или сети с помощью различных методик разведки и обнаружения, в то время как защитникам обычно не хватает разведданных о своих противниках. Чтобы компенсировать такие ассиметричные условия,

команда защиты может использовать технологии обмана злоумышленника, существенно улучшая противостояние угрозам [6,7].

Стратегия защиты с использованием традиционных инструментов безопасности, таких как брандмауэры, средства контроля аутентификации и системы предотвращения вторжений (IPS), бывает не всегда эффективна, когда речь заходит о направленных и хорошо спланированных атаках. Даже при использовании стратегии глубоко эшелонированной защиты [8], когда по всей целевой сети размещены несколько уровней средств контроля безопасности, команде защиты по-прежнему трудно предотвращать и обнаруживать хорошо спланированные и подготовленные атаки (APT). Атаки такого типа обычно используют уязвимости нулевого дня для установления опорных точек внутри целевой сети и при этом оставляют мало следов своей деятельности. Из-за этого обнаружение таких атак становится непростой задачей. Более того, классические решения для обнаружения аномалий в сети, такие, как системы обнаружения вторжений (IDS), могут генерировать большое количество ложных предупреждений, в результате чего взгляд сотрудника безопасности может быть замылен, он может пропустить действительно важное предупреждение. Технологии обмана, использующиеся в защитных целях, позволяют обнаруживать уязвимости нулевого дня, гарантируют минимальное количество ложных срабатываний и могут выступать в качестве дополнительного уровня защиты для улучшения её качества и нивелирования слабых сторон [9-11].

Как было написано выше, воздействие на восприятие (в нашем случае злоумышленника) является сильным инструментом в руках команды защиты. Методика построения защиты на основе обмана фокусируется в первую очередь не на исследовании действий атакующего в тот момент, когда он уже пробрался во внутреннюю сеть и взаимодействует с настоящими активами организации, а на попытке его обмануть, скрыть настоящую поверхность

атаки [12]. Цель состоит в том, чтобы скрыть критические активы от злоумышленников и запутать их, тем самым увеличить риск их обнаружения, заставив их использовать потенциал своей атаки на ложных активах, теряя время и тратя ресурсы. Таким образом, эффективность атаки злоумышленника может быть значительно уменьшена, ведь он потратит свое время на взаимодействие с ложным активом, а также продемонстрирует свой арсенал, возможно раскроет свою истинную цель [13]. Методику построения защиты, основанную на обмане, можно считать проактивной в отличии от классической пассивной защиты, потому что злоумышленник идет по сценарию, который заготовила команда защиты заранее. Её ключевым элементом также является упреждение атаки до того, как она произойдет, за счет инфраструктуры ложных целей [14].

С начала развития истории обмана злоумышленника с помощью Honeypot, было изобретено большое количество разных видов ловушек. Классифицированы эти ловушки могут быть по разным принципам, пример классификации представлен на рисунке 1 [15-17].

Несмотря на различные виды, все ловушки имеют одно и то же предназначение – быть подвергнутыми атаке [18]. Несколько взаимосвязанных ловушек honeypots образуют сеть ловушек honeynet. При развитии стратегии honeynet, появилась возможность создавать инфраструктуру, собранную только из ловушек, при этом максимально похожую на настоящую сеть, способную запутать злоумышленника на длительное время. В технологиях обмана используются не только ловушки, но и приманки (например, учетные записи, файлы пользователей, записи в базе данных и пароли), их можно в совокупности назвать honeytokens. На русский можно перевести как «хлебные крошки» (их мы разбрасываем по инфраструктуре, их находит и на них клюёт злоумышленник). Эти файлы приманки контролируются с помощью отдельного сервера (например,

HoneyComb в Deja Vu [19]) и как только к ним будет получен доступ, сервер отправит сигнал тревоги, предупреждающий о возможном вторжении. Такой сценарий возможен благодаря развитию технологий программ проверки целостности по типу Tripwire, которые дают возможность контролировать файловые системы и проверять, были ли они изменены, удалены, перемещены или добавлены. Таким образом получается, что злоумышленник может столкнуться с ловушкой или приманкой на каждом этапе своего перемещения в сети, если он не выберет правильную цель, то он будет обнаружен [20].

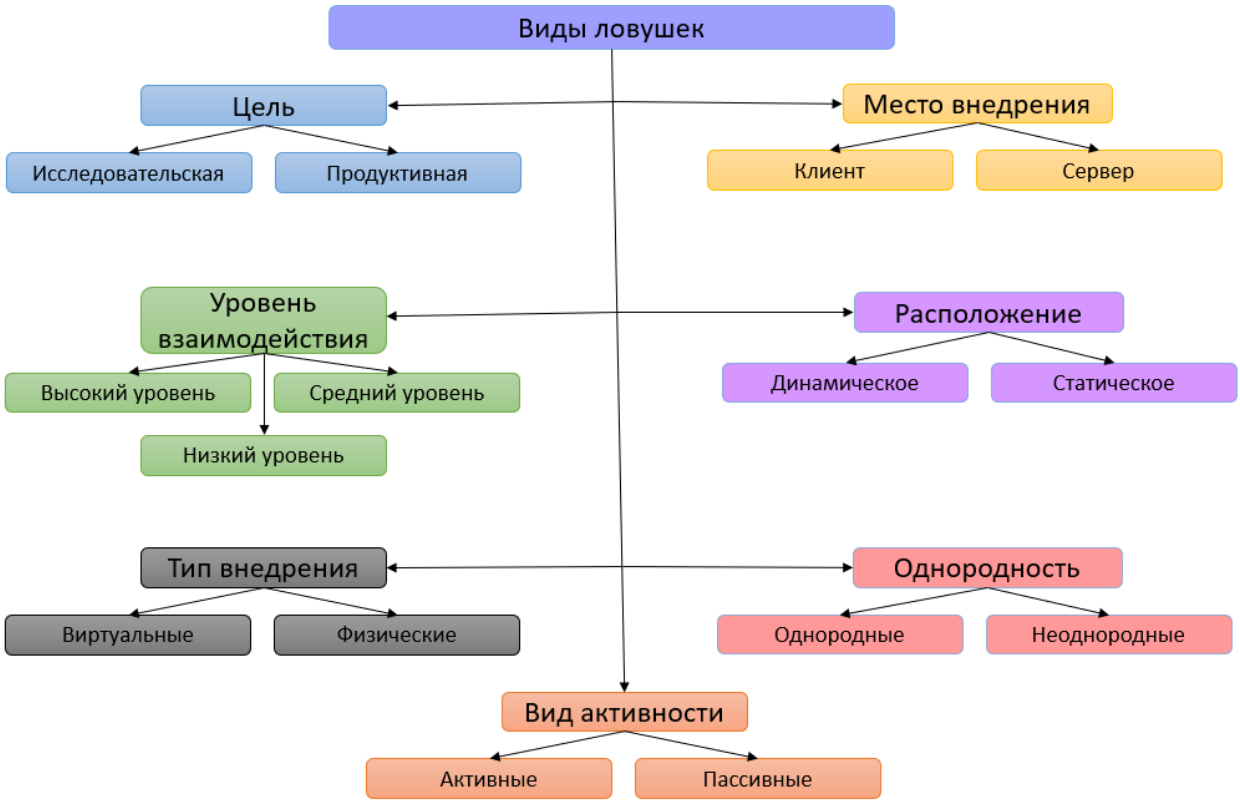

Рис. 1 – виды ловушек

Тем не менее, если honeypots и honeytokens останутся со статичными размещением и конфигурациями, у противника будет достаточно времени, чтобы сделать вывод об их существовании, установить их место нахождения и получить возможность миновать их при развитии своей атаки [21]. Более

того, ловушки, особенно с высоким уровнем взаимодействия, которые предлагают доступ к операционной системе, могут быть использованы злоумышленником для дальнейшего получения привилегированного доступа и использованы в качестве опорной точки для компрометации других систем в сети [22]. Именно здесь на первый план выходит защита с помощью перемещения целей (moving target defense, MTD), методы MTD обеспечивают обман злоумышленника посредством рандомизации и реконфигурации сетей, активов и инструментов защиты [23]. Благодаря динамическому изменению расположения реальных и поддельных активов, поверхности атаки критически важных ресурсов может быть максимально запутана. При этом злоумышленник будет сбит с толку, что существенно замедлит его продвижение в сети. В своей работе Фрэн Коэн приводит исследование, в котором принимали участие группы слабо, средне и хорошо подготовленные специалисты по проникновению в сеть организации. Целью злоумышленников было найти ключевой актив в организации. Для противодействия им использовались ловушки, приманки и методы перемещения MTD. Итоги исследования были следующие – добавление методов MTD к методам использования ловушек и приманок существенно увеличивало время поиска целевого актива, что доказывало эффективность их применения [24].

Ловушки

Ловушки можно разделить на две категории: исследовательские и производственные (продуктивные) [25]. Исследовательские ловушки собирают информацию об атаках, располагаясь за периметром организации, благодаря чему они позволяют исследовать современные угрозы, не переживая о проникновении злоумышленника во внутреннюю сеть. Благодаря полученным с таких ловушек данным, появляется возможность

улучшения существующих методов защиты. Тем не менее, они не помогут в тот момент, когда злоумышленник уже проник во внутреннюю сеть. На смену им приходят производственные ловушки, которые сосредоточены на выявлении злоумышленника внутри сети [26].

Далее речь пойдет про производственные ловушки, про стратегии их размещения внутри сети, а также про методы остановки атак с их помощью. Существует несколько стратегий по размещению ловушек и приманок в сети, вот некоторые из них: sacrificial lamb, hacker zoo, minefield, proximity decoys, redirection shield, deception ports. В свободном авторском переводе, стратегии будут звучать следующим образом: жертвенный ягненок, хакерский зоопарк, минное поле, ловушки при сближении, экран перенаправления, порты обмана [27]. Описание стратегий приведено на рисунке 2.

Стратегия	Описание
Жертвенный ягненок	Изолированная система, не имеющая доступа к производственным системам
Хакерский зоопарк	Целая подсеть, состоящая из ловушек в виде различных платформ со своими сервисами, уязвимостями и конфигурациями, изолированная от основной сети
Минное поле	Ловушки, расставленные около по контуру внутренней сети. Они должны служить защитой на дальнем рубеже.
Ловушки при сближении	Несколько ловушек, размещенные перед ценным активом организации, злоумышленник должен сперва взаимодействовать с ними
Экран перенаправления	Внешние приманки, которые появляются в производственных системах благодаря перенаправлению портов
Порты обмана	Имитация служб (например, SMTP, DNS, FTP) в производственных системах

Рис. 2 – стратегии обмана ловушками

Стратегия жертвенного ягненка была изобретена первой К. Столлом [4] и описана в его статье еще в 1989 году. Эта стратегия проста и понятна – её идея заключается в разворачивании машины ловушки в сети для обнаружения злоумышленника. У такой стратегии есть минус – поскольку ловушка получается изолированной от производственных систем, при использовании такой стратегии существенно увеличивается шанс обнаружения ловушки злоумышленником. Продолжением идеи стратегии жертвенного ягненка является стратегия хакерского зоопарка, где используется подсеть, состоящая из ловушек - жертвенных ягнят. Она имеет схожие минусы, и опытный злоумышленник также сможет определить подсеть ловушки [28]. Honeypots, развернутые по стратегии «Минное поле», размещаются по периметру сети [29,30]. Для обеспечения полной безопасности в сети также размещаются системы обнаружения вторжений (IDS) и сканеры уязвимостей. Но вместо того, чтобы следить за рабочими серверами, эти IDS и сканеры уязвимостей фокусируются на ловушках. Таким образом, вероятность ложных срабатываний значительно снижается. В качестве примера можно привести LaBrea и Honeyd, используемые в замаскированном режиме, а также Mantrap [31]. Следующие стратегии «ловушка при сближении» (с ключевой инфраструктурой) и «экран перенаправления» используются для того, чтобы запутать злоумышленника и увести его подальше от критически важных активов. Ловушка при сближении подразумевает непосредственное наличие её в сети с производственной инфраструктурой, что является основным отличием. В связи с этой особенностью, стратегия «экран перенаправления», работающая на перенаправлении трафика и портов, обладает большей гибкостью в сравнении. Развертывание портов ловушек можно считать последним рубежом защиты. Эти ловушки имитируют уязвимые сервисы (показывая доступные порты для подключения к ним) и могут быть использованы даже в

том случае, если злоумышленник уже добрался до ключевого актива и начинает его изучение [32].

Приманки

Приманки служат для того, чтобы, будучи предоставлены злоумышленнику, заставить его их использовать, тем самым раскрыв себя. Эти приманки следует оставлять по всей сети, а также четко определять места расположения каждой из них, чтобы понимать, откуда злоумышленник смог украсть ложные данные [33].

Пароли-приманки: используются для реальных или ложных учетных записей. Их идея заключается в том, чтобы заставить злоумышленника ввести заранее сгенерированный ненастоящий пароль, при вводе которого сработает система безопасности и уведомит о наличии нарушителя. При этом такие пароли можно генерировать по несколько штук для каждой учетной записи [34], в результате чего злоумышленник не сможет понять, какой пароль является настоящим, даже если сможет получить их из хэшей.

Ложные данные в базе данных: в базу данных можно внедрить приманку, которая будет привлекать внимание злоумышленников [35]. Такой приманкой могут стать такие объекты как TABLE CREDIT_CARDS или VIEW EMPLOYEES_SALARY. В том случае, если эти объекты будут использоваться, команда защиты получит уведомление о проводимой атаке. Для большей эффективности, следует использовать очень похожие на реальные данные. В том случае, если реалистичное заполнение такими данными может занять существенное количество времени, можно использовать автоматизированные инструменты, которые автоматически проводят анализ базы данных и её элементов, в результате чего способны генерировать похожие данные. Такой особенностью обладает HoneyGen [36].

Файлы приманки: в большинстве систем, позволяющим создавать

инфраструктуру ложных целей, есть возможность использования файлов приманок (например, в Open Source решении Deja Vu) [19]. Для использования файлов приманок требуются 2 составляющие – сгенерированная приманка, а также сервис, который будет отслеживать в сети её перемещение, изменение, взаимодействие с ней. В роли приманок могут выступать самые различные файлы, но, чаще всего, ими могут быть файлы Word, Excel, PowerPoint, PDF [37,38]. Чтобы обеспечить возможность обнаружения, можно встраивать в файлы-приманки различные виды защиты:

1) уникальный водяной знак, который может быть обнаружен при загрузке файла в память или при появлении его в сетевом трафике;

2) маячок, который будет сигнализировать удаленному веб-серверу об открытии файла;

3) данные honeytokens по типу ложных паролей. Использование этих данных вызовет срабатывание системы безопасности [39].

Для того, чтобы увеличить привлекательность приманок, они должны быть развернуты в тех местах, где действительно могли бы присутствовать (этот процесс возможно автоматизировать, используя анализатор инфраструктуры и файловой системы) [40]. Вместе с этим, сам файл должен быть похож на реальный, содержать схожие с реальным файлом данные. В этой сфере есть пространство для изучения и анализа. Дело в том, что на текущий момент генерация ложного файла, в котором имели бы место настоящие данные, возможно с помощью использования схожих файлов и смены мест информации в них [41]. Де факто получатся, что изменение положения слов в файле может не привести к успешной маскировке данных, либо наоборот не привлечь злоумышленника к изучению этого файла. Если же использовать искусственный интеллект для генерации файла определенного типа (например, финансовый отчет или коммерческое предложение), то он может выйти более правдоподобным. Если мы сделаем

приманку, которая будет похожа на ключевой файл, который является целью злоумышленника, и он будет аналогичен настоящему, но содержать совершенно другие данные, то получится обмануть злоумышленника на более длительное время. Если файл будет качественный, и злоумышленник поверит, что он добрался до цели своей атаки, возможно он приостановит атаку на время изучения файла, что подарит больше времени команде защиты [42]. Есть возможность генерации ложных системных файлов, которые скрыты от обычного пользователя, но могут быть злонамеренно использованы злоумышленниками. Такие файлы позволяют практически полностью избежать фантомных срабатываний, но при этом выловить злоумышленника [43, 44].

Перемещение целей

Как и было описано выше, стратегия перемещения целей является одной из ключевых стратегий при обмане злоумышленника. Методы MTD направлены на рандомизацию сетевых компонентов. Благодаря этим методам, снижается вероятность успешной атаки, увеличивается динамичность компонентов сети, уменьшается вероятность получить значительный ущерб от реализации атаки [45,46]. Таким образом, перемещение целей увеличивает неопределенность в сети для злоумышленника, заставляя тратить его большее количество ресурсов для корректного взаимодействия с сетью. Стратегия делает сеть менее детерминированной и однородной. Что касается методик, который могут быть применены в рамках этой стратегии, то можно выделить следующие:

1) Обфускация IP. Термин обфускация означает делать неочевидным, запутанным, сбивать с толку. Обфускация IP-адресов — это процесс сокрытия или маскировки местоположения пользователя. Обфускация IP-адресов, которая также известна как геоспуфинг, включает в себя все, что

позволяет скрыть или обезличить личность пользователя с помощью различных методов. Чтобы злоумышленники не могли отслеживать хосты в целевой сети на основе IP-адресов, был предложен ряд методов обфускации IP [47]. Например, может использовано динамическое преобразование сетевых адресов (DyNAT), представляющее собой метод обфускации протокола, который может поменять местами IP-адреса источника и назначения в заголовках пакетов. Также может быть использована рандомизация сетевого адресного пространства (NASR), которая модифицирует DHCP-сервер таким образом, что он выдает IP адреса на короткое время, в результате чего IP-адреса хост-машин часто меняются. Большое количество других методов, не описанных выше, основаны на случайном изменении IP-адресов [48].

2) Обфускация ОС. Для защиты от атак с использованием цифровых отпечатков (fingerprints) операционной системы можно использовать метод на основе SDN, который скрывает информацию об операционной системе в случае обнаружения нелегитимного трафика. Регулярное изменение цифровых отпечатков также поможет избежать обнаружения целевого устройства и запутает злоумышленника [49].

3) Использование динамических систем. Еще одним часто используемым методом является рандомизация расположения адресного пространства (Address space layout randomization, ASLR) [50]. Этот метод препятствует использованию уязвимостей памяти путем рандомизации адресов памяти загруженного ПО, то есть метод препятствует повреждению этой памяти. Для устранения атак с использованием кода-инъекции можно использовать рандомизацию набора команд (ISR), при котором закодированная версия команд загружается в память и будет декодирована ключом перед выполнением [51]. Возможности злоумышленников во многом зависят от наличия уязвимостей в конкретных ОС или процессорах. Одна из

методик запутывания злоумышленника предлагает использовать в сети различные операционные системы, чтобы злоумышленнику было сложнее работать с сетью, и он не имел универсального ключа для всех машин. Метод может быть реализован с помощью нескольких виртуальных машин, которые хранят общие данные в базе данных. Доступ к ним будет ротироваться, только одна из этих машин будет иметь IP адрес, с которым можно будет взаимодействовать. Периодическая ротация выделения IP адресов контролируется с помощью компьютера администратора, в случае обнаружения вторжения на одну из машин ротации, она вычеркивается из списка и больше не получает IP-адреса, а следовательно, и возможности взаимодействовать с ней. Похожий подход можно использовать не с данными, а с приложениями, делая снимки текущих состояний и перенося их на другие виртуальные машины сети, закрывая доступ к атакованным. [52]

4) Использование динамического ПО. Существует большое количество разных атак, использующих уязвимости программного обеспечения [53, 54]. Их эффективность зависит от понимания используемого ПО на машине жертвы, а также наличия уязвимостей в этом ПО. Используя обфускацию ПО, защищающаяся сторона может повысить неопределенность в конкретной цели, увеличить затраты злоумышленников и обеспечить эффективное противодействие атакам по побочным каналам [55]. Один из методов предлагает разделить сложную программу на более мелкие составляющие части, каждая из которых имеет набор исполняемых вариантов, функционально идентичных, но с разными качественными характеристиками (например, производительностью и надежностью). Затем исполняемые варианты могут быть перемешаны, тем самым изменив поверхность атаки и добавив неопределенности.

Анализ существующих методов MTD показал, что, хотя они и способны обмануть злоумышленников, методы MTD имеют практические

ограничения при применении в реальных условиях, особенно если речь идет об облачных ресурсах. К этим ограничениям относятся:

-Увеличенная трата ресурсов (вычислительных мощностей, административных ресурсов, лицензий и т.д.)

-Растущая сложность управления. Чем больше дополнительных методов и функций MTD планируется к использованию, чем более кастомизируемыми они являются, тем сложнее управлять в итоге стратегией, поддерживать её, адаптировать под новые задачи информационной безопасности.

-Потенциальное увеличение сложности атаки, под которую придется адаптировать стратегию [56].

Deception platform

Стратегия использования ловушек и приманок с целью защиты сети организации получила свое дальнейшие развитие в виде стратегии Deception и реализацию как средства защиты в виде Distributed Deception Platform (DDP). Deception также базируется на использовании ловушек и приманок, но имеется несколько важных отличий:

1) Honeypot размещают около ценных активов в сети организации, технология Deception предполагает размещение ловушек и приманок по всей инфраструктуре.

2) Технология Deception качественно имитирует реальную инфраструктуру организации, благодаря чему увеличивается шанс не только привлечь злоумышленника, но и запутать его, заставить думать, что он взаимодействует с реальными активами.

3) Honeypot сложно, медленно и дорого масштабировать, в то время как ловушки и приманки технологии Deception могут быть развернуты автоматически или полуавтоматически из единого окна управления.

4) Технология Deception предполагает меньшее количество ложных срабатываний за счет сокрытия ложной инфраструктуры от обычных пользователей.

5) Технология Deception предлагает больший уровень автоматизации и позволяет проще анализировать состояния ловушек и приманок, проводя наблюдения за всеми ложными активами в едином окне [57].

Deception Platform – это централизованно управляемые системы для организаций, предназначенные для создания, распространения и управления всей обманчивой средой и связанными с ней архитектурными элементами, которые часто виртуализируются и по существу неотличимы от реальных активов и используются в качестве приманки для привлечения и обнаружения злоумышленника [57]. Одновременное применение технологий MTD и Deception может значительно увеличить вероятность обмана злоумышленника благодаря инфраструктуре ложных целей и динамическому изменению ложных и настоящих целей, причем управлять ненастоящей инфраструктурой, мониторить её и разворачивать новые ловушки и приманки можно из одного места [58].

В настоящее время самой современной стратегией является Deception, она сочетает в себе ловушки и приманки разных видов, необходимых для выполнения разных задач по защите сети [59]. Ловушки, которые в ней используются, предназначены для противодействия злоумышленнику внутри сети (то есть они производственные). Они создают минимальное количество ложных срабатываний, при этом технология позволяет из единого места оперативно разворачивать ловушки. Они могут быть разных форматов, как правило, платформы обмана могут быть адаптированы под задачи заказчика, добавляя в спектр доступных ловушек и приманок специализированные. Например, сетевую имитацию какого-нибудь производственного оборудования, характерного для организации заказчика. Ловушки эти могут

варьироваться в зависимости от возможности взаимодействия с ними (высоко интерактивные, средние и низко интерактивные), формировать целые ложные сети и маскироваться под реальные активы. Использование MTD в данном случае увеличит вероятность запутать злоумышленника, а автоматизация MTD позволит быстро внедрять целый ландшафт новых ловушек и приманок в случае необходимости таким образом, чтобы злоумышленнику стало еще сложнее найти настоящий актив.

Таким образом, наиболее целесообразным вариантом из различных средств обмана является использование Deception платформы с богатым арсеналом ловушек и приманок, а также применение техник MTD для ложной и настоящей инфраструктуры.

Заключение

В результате проведенного исследования были выявлены основные на сегодняшний день технологии, позволяющие обмануть злоумышленника. Данная обзорная статья является первой статьей на русском языке, которая собирает воедино технологии обмана злоумышленника, включая ловушки honeypot, приманки honeytoken, перемещение целей MTD, платформу обмана Deception, объясняет разницу между ними, применение каждой из них и приводит историю развития от единичных ловушек, раскиданных по стратегии жертвенного ягненка, до комплексной платформы обмана. В результате изученных материалов при формировании статьи, были выявлены основные виды ловушек, а также стратегии, в соответствии с которыми ловушки могут быть расположены в сети. Было описано целевое назначение каждой указанной стратегии размещения ловушек, основной фокус делался на стратегиях размещения продуктивных ловушек. Были описаны различные виды приманок, а также методики их работы для обмана злоумышленника с примерами. Приманки могут взаимодействовать с ловушками, усиливая

воздействие обмана злоумышленника. Эта идея дала возможность соединить работу ловушек и приманок в единой стратегии, на единой платформе – Deception платформе. Эта платформа имеет явные преимущества по сравнению с отдельными ловушками и приманками, они были описаны в статье. Чтобы уменьшить вероятность закрепления злоумышленника на ловушке и дальнейшего его продвижения по сети, используя ловушку как опорный пункт, можно применять техники перемещения целей в сети. Они показывают хорошую работу вместе с ловушками (в том числе с платформой Deception), подтверждающие это исследования были приведены в статье.

Таким образом, обман злоумышленника является хорошим средством для выстраивания проактивной защиты и позволяет уменьшить преимущество злоумышленника во время проведения атаки. Богатый арсенал ловушек разных видов позволяет узнавать о злоумышленнике большое количество информации. Обман злоумышленника может произойти до момента его захода внутрь сети, на дальних рубежах внутри сети или около ценных активов. Приманки также имеют значительный спектр различных видов и позволяют выявить злоумышленников на разных этапах его атаки. Deception платформы являются относительно новым веянием в сфере обмана злоумышленников и уже зарекомендовали себя как надежный инструмент защиты, создающий минимальное количество ложных срабатываний и предоставляющий наиболее ценную информацию о злоумышленнике. MTD методы, хоть и имеют ограничения, но могут быть использованы эффективно с ловушками, приманками и Deception-платформами, увеличивая время, требуемое злоумышленнику для достижения конечной цели.

Литература

1. 2019 Data Breach Investigations Report. URL: verizon.com/business/resources/en/reports/2019-data-breach-investigations-report.pdf (дата обращения: 04.11.2024).

2. Coronavirus-themed phishing attacks and hacking campaigns are on the rise. URL: zdnet.com/article/coronavirus-themed-phishing-attacks-and-hacking-campaigns-are-on-the-rise/ (дата обращения: 02.11.2024).

3. Хохолева Е.А. Обман как средство манипулирования сознанием. // «Дискуссия» журнал научных публикаций, 2012, №11 (29), С. 151-155. URL: cyberleninka.ru/article/n/obman-kak-sredstvo-manipulirovaniya-soznaniem-k-postanovke-problemy-v-sfere-upravleniya-personalom (дата обращения: 10.11.2024).

4. Stoll C., Malina R. The Cuckoo's Egg: Tracking a Spy through a Maze of Computer Espionage // Computer Science, 1991. DOI: doi.org/10.2307/1575326

5. Lynn III W. J. Defending a New Domain: The Pentagon’s Cyberstrategy, // Foreign Affairs, vol. 89, 2010, no. 5, pp. 97–108, URL: jstor.org/stable/20788647 (дата обращения: 09.11.2024)

6. Ferguson-Walter K., Fugate S., Mauger J., Major M. Game theory for adaptive defensive cyber deception, // in Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security - HotSoS ’19. Nashville, Tennessee: ACM Press, 2019, pp. 1–8. DOI: doi.org/10.1145/3314058.3314063

7. Shade T., Rogers A., Ferguson-Walter K., Elsen S. B., Fayette D., Heckman K. The Moonraker Study: An Experimental Evaluation of Host-Based Deception, // in Hawaii International Conference on System Sciences, 2020. URL: pdfs.semanticscholar.org/4f80/8f74597b214bc39a79616c2ab564fd629f55.pdf (дата обращения: 10.11.2024)

8. Коломойцев В.С. Построение эшелонированных систем защиты информации. // Первая Всероссийская научная конференция. Санкт-Петербург, 2020, С. 190-192, DOI: doi.org/10.31799/978-5-8088-1452-3-2020-1-190-192, -EDN: YOXMVF

9. Javadpour Amir, Ja'fari Forough, Taleb Tarik. A comprehensive survey on cyber deception techniques to improve honeypot performance // Computers & Security, Volume 140, 2024. DOI: doi.org/10.1016/j.cose.2024.103792

10. Jorquera J.M. Identification and classification of cyber threats through SSH honeypot systems // Handbook of Research on Intrusion Detection Systems, 2020, pp. 105-129. DOI: dx.doi.org/10.4018/978-1-7998-2242-4

11. Javadpour A. Dmaidps: a distributed multi-agent intrusion detection and prevention system for cloud iot environments // Cluster Computing, February Volume 26, Issue 1, 2023, pp. 367-384 DOI: doi.org/10.1007/s10586-022-03621-3

12. Almeshekah M.H., Spafford E.H. Cyber security deception // Cyber Deception, Springer, 2016, pp. 25-52. DOI: doi.org/10.1007/978-3-319-32699-3_2

13. Ross R., Pillitteri V., Graubart R., Bodeau D., McQuaid R. Developing cyber resilient systems: A systems security engineering approach // National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep. NIST SP 800-160v2, Nov. 2019. DOI: doi.org/10.6028/NIST.SP.800-160v2r1

14. Anwar A.H., Kamhoua C.A., Honeypot Allocation for Cyber Deception under Uncertainty // IEEE Transactions on Network and Service Management, Volume 19, Issue 3, 2022, pp. 3438-3452. DOI: doi.org/10.1109/TNSM.2022.3179965

15. Javadpour A., Taleb T., Ja'Fari F., A comprehensive survey on cyber deception techniques to improve honeypot performance // Computers & Security, Volume 140, 2024, №103792, DOI: doi.org/10.1016/j.cose.2024.103792

16. Onyekware U. Cutting Edge Trends in Deception Based Intrusion Detection Systems—A Survey // Journal of Information Security, 2021, pp. 250-269. DOI: doi.org/10.4236/jis.2021.124014

17. Salimova H.R., A virtual honeypot framework // Central Asian Research Journal for Interdisciplinary Studies, Volume 2, Issue 5, 2022, pp. 479-486. URL:

researchgate.net/publication/221260586_A_Virtual_Honeypot_Framework (дата обращения: 08.11.2024)

18. Spitzner L. Honeypots: Tracking Hackers // Boston: Addison-Wesley Professional, Sep. 2002. URL: theswissbay.ch/pdf/Gentoomen%20Library/Security/0321108957.Addison-Wesley%20Professional.Honeypots-%20Tracking%20Hackers.pdf (дата обращения: 10.11.2024)

19. DejaVU - Open Source Deception Platform. URL: github.com/bhdresh/Dejavu (дата обращения: 01.11.2024)

20. Конкин Ю.В. Анализ особенностей построения систем защиты информации от несанкционированного доступа на основе ложных информационных систем // VII Международный научно-технический форум СТНО-2024. Сборник трудов. Том 3, С. 167-171. EDN: UZZJOA.

21. Ayeni O., Alese B., Omotosho L. Design and implementation of a medium interaction honeypot // International Journal of Computer Applications., Volume 70, 2013, №20. DOI: dx.doi.org/10.5120/12197-8136

22. Spitzner Lance Honeypots: Catching the insider threat // Security Focus information, Jan. 2004. DOI: dx.doi.org/10.1109/CSAC.2003.1254322.

23. Pawlick J., Colbert E., Zhu Q. A Game-Theoretic Taxonomy and Survey of Defensive Deception for Cybersecurity and Privacy // ACM Computing Surveys, Volume 52, Issue 4, 2019, DOI: doi.org/10.1145/3337772.

24. Crouse M., Prosser B. Probabilistic Performance Analysis of Moving Target and Deception Reconnaissance Defenses // 2nd MTD@CCS conference, 2015, pp. 21-29. DOI: doi.org/10.1145/2808475.2808480

25. Как будто мёдом намазано: что такое Honeypot и как поймать хакера «на живца». URL: securitylab.ru/analytics/536141.php (дата обращения: 03.11.2024)

26. Bringer M.L., Chelmecki C.A. Recent advances and future trends in honeypot research // International Journal of Computer Network and Information Security, Volume 4, 2012, № 10, p. 63. DOI: dx.doi.org/10.5815/ijcnis.2012.10.07

27. Scottberg B., Yurcik W., and Doss D. Internet honeypots: Protection or entrapment? // in IEEE International Symposium on Technology and Society (ISTAS'02). Raleigh, NC, USA: IEEE, 2002, pp. 387–391. DOI: dx.doi.org/10.1109/ISTAS.2002.1013842

28. Liu G., Ou X., Singhal A., Tabari A.Z. Revealing human attacker behaviors using an adaptive Internet of things honeypot ecosystem // 19ep IFIP International Conference on Digital Forensics, 2023, pp. 73-90. DOI: dx.doi.org/10.1007/978-3-031-42991-0_5

29. Doubleday H. SSH Honeypot: Building, Deploying and Analysis // International Journal of Advanced Computer Science and Applications, 2016, Vol. 7, No. 5, pp. 117-121. DOI: dx.doi.org/10.14569/IJACSA.2016.070518

30. Gibbens M., Rajendran H. Honeypots // The University of Arizona, 2012, pp. 1-12. URL: www2.cs.arizona.edu/~collberg/Teaching/466-566/2013/Resources/presentations/2012/topic12-final/slides.pdf (дата обращения 10.11.2024)

31. Ochiai H., Honeyboost: Boosting honeypot performance with data fusion and anomaly detection // Expert Systems with Applications, Volume 201, September 2022, № 117073. DOI: doi.org/10.1016/j.eswa.2022.117073

32. Bilinski, M., Gabrys, R. Optimal placement of honeypots for network defense // 9th International Conference on Decision and Game Theory for Security, Volume 11199 LNCS, 2018, pp. 115-126. DOI: dx.doi.org/10.1007/978-3-030-01554-1_7

33. Ja'fari F., An intelligent botnet blocking approach in software defined networks using honeypots // Journal of Ambient Intelligence and Humanized

Computing, Volume 12, Issue 2, 2021, pp. 2993-3016. DOI: dx.doi.org/10.1007/s12652-020-02461-6

34. Juels A, Rivest R. L. Honeywords: Making password-cracking detectable, // in Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security - CCS '13. Berlin, Germany: ACM Press, 2013, pp. 145–160. DOI: doi.org/10.1145/2508859.2516671

35. Pedersen J.M., Srinivasa S. Interaction matters: a comprehensive analysis and a dataset of hybrid IoT/OT honeypots // 38th Annual Computer Security Applications Conference, 2022, pp. 742-755. DOI: doi.org/10.1145/3564625.3564645

36. Bercovitch M., Renford M., Hasson L., Shabtai A., Rokach L. HoneyGen: An automated honeytokens generator // in Proceedings of 2011 IEEE International Conference on Intelligence and Security Informatics, Jul. 2011, pp. 131–136. DOI: dx.doi.org/10.1109/ISI.2011.5984063

37. Neal C. Attacker Attribution via Characteristics Inference Using Honeypot Data // 16th International Conference on Network and System Security, 2022, pp. 155-169. DOI: dx.doi.org/10.1007/978-3-031-23020-2_9.

38. Yuan J., Yang H., Kong Y. A highly interactive honeypot-based approach to network threat management // Future Internet, Volume 15, 2023, № 4, p. 127. DOI: doi.org/10.3390/fi15040127

39. Padayachee K. Aspectising honeytokens to contain the insider threat // IET Information Security, vol. 9, no. 4, 2014, pp 240–247. DOI: doi.org/10.1049/iet-ifs.2014.0063

40. Voris J., Jermyn J., Keromytis A. D., Stolfo S. J. Bait and Snitch: Defending Computer Systems with Decoys // Proceedings of the Cyber Infrastructure Protection Conference, Strategic Studies Institute, 2013, p. 25.DOI: doi.org/10.7916/D8RN3H9S

41. Whitham B. Automating the Generation of Enticing Text Content for High-Interaction Honeyfiles // IEEE computer society, 2017. DOI: doi.org/10.24251/HICSS.2017.733

42. Lim C., Budiarto E., Hobert K. Enhancing Cyber Attribution through Behavior Similarity Detection on Linux Shell Honeypots with ATT&CK Framework // 1st IEEE International Conference on Cryptography, Informatics, and Cybersecurity, 2023, pp. 139-144. DOI: doi.org/10.1109/ICoCICs58778.2023.10276639

43. Yamin M.M., Katt B. Use of cyber attack and defense agents in cyber ranges: A case study // Computers & Security, Volume 122, 2022, № 102892, DOI: doi.org/10.1016/j.cose.2022.102892

44. Lee J., Choi J., Lee G., Shim S-W., Kim T. Phantom FS: FileBased Deception Technology for Thwarting Malicious Users, // IEEE Access, vol. 8, 2020, pp. 32 203–32 214. DOI: dx.doi.org/10.1109/ACCESS.2020.2973700

45. Соколовский С.П. Moving target defense for securing Distributed Information Systems // Информатика: проблемы, методология, технологии, Сборник материалов XIX международной научно-методической конференции, 2019, С.639-643 -EDN: ZFDMBF

46. Liu G., Ou X., Singhal A., Tabari A.Z. Revealing human attacker behaviors using an adaptive Internet of things honeypot ecosystem // 19ep IFIP International Conference on Digital Forensics, 2023, pp. 73-90 DOI: dx.doi.org/10.1007/978-3-031-42991-0_5

47. Zubaida R. Proactive defense mechanism: Enhancing IoT security through diversity-based moving target defense and cyber deception // Computers & Security, Volume 139, 2024. DOI: doi.org/10.1016/j.cose.2023.103685

48. Vitor A., TOTP Moving Target Defense for sensitive network services // Pervasive and Mobile Computing Volume 74, 2021. DOI: doi.org/10.1016/j.pmcj.2021.101412

49. Wei D. Obfuscation mechanism for simultaneous public event information release and private event information hiding in discrete event systems // Information Sciences, Volume 690, 2024. DOI: doi.org/10.1016/j.ins.2024.121554

50. Li L., Just J. Address-Space Randomization for Windows Systems // Annual Computer Security Applications Conference (ACSAC'06), 2006, pp. 329–338. DOI: doi.org/10.1109/ACSAC.2006.10

51. Zhang Li, Thing L. Three Decades of Deception Techniques in Active Cyber Defense - Retrospect and Outlook // Computers & Security, Volume 106, 2021, №102288, DOI: doi.org/10.1016/j.cose.2021.102288

52. Okhravi H., Comella A. Creating a Cyber Moving Target for Critical Infrastructure Applications // International Conference on Critical Infrastructure Protection, Advances in Information and Communication Technology, 2011, pp. 107–123. DOI: doi.org/10.1016/j.ijcip.2012.01.002

53. Carlo A. Cyber-attacks on critical infrastructures and satellite communications // International Journal of Critical Infrastructure Protection, 2024 DOI: doi.org/10.1016/j.ijcip.2024.100701

54. Eng S., How K.C., Zhu Y. Honeypot for cybersecurity threat intelligence // Conference on Science, Engineering and Technology, 2023, pp. 587-598. URL: link.springer.com/chapter/10.1007/978-981-19-7222-5_44 (дата обращения: 07.11.2024)

55. Larsen P., Homescu A., Brunthaler S., Franz M. SoK: Automated Software Diversity // Symposium on Security and Privacy, 2014, pp. 276–291. DOI: dx.doi.org/10.1109/SP.2014.25

56. Kang K.W SD-MTD: software-defined moving-target defense for cloud-system obfuscation // KSII transactions on internet and information systems, 2022, pp. 1063-1075. URL: syscore.sejong.ac.kr/~woongbak/publications/J38.pdf (дата обращения: 04.11.2024)

57. Путято М.М., Макарян А.С., Чич Ш. М., Маркова В.К. Исследование применения технологии Deception для предотвращения угроз кибербезопасности // Прикаспийский журнал: управление и высокие технологии, 2020, № 4 (52), С. 85-98. EDN: QXGGTW. DOI: doi.org/10.21672/2074-1707.2020.52.4.085-098

58. Тихонов А.М. Платформа для создания распределенной инфраструктуры ложных целей как часть эшелонированной системы защиты // Известия Института Инженерной Физики, 2024, №3, С. 65-71. EDN: QSVNKO

59. Alissa K., Alqahtani M., Faiz T., Alyas T. Multi-cloud integration security framework using honeypots // Mobile Information Systems, 2022, pp. 1-13. DOI: doi.org/10.1155/2022/2600712

References

1. 2019 Data Breach Investigations Report. URL: verizon.com/business/resources/en/reports/2019-data-breach-investigations-report.pdf

2. Coronavirus-themed phishing attacks and hacking campaigns are on the rise. URL: zdnet.com/article/coronavirus-themed-phishing-attacks-and-hacking-campaigns-are-on-the-rise

3. Hoholeva E.A. «Diskussija» zhurnal nauchnyh publikacij, 2012, №11 (29), pp. 151-155. URL: cyberleninka.ru/article/n/obman-kak-sredstvo-manipulirovaniya-soznaniem-k-postanovke-problemy-v-sfere-upravleniya-personalom

4. Stoll C., Malina R. Computer Science, 1991. DOI: doi.org/10.2307/1575326

5. Lynn III W. J. Foreign Affairs, 2010. vol. 89, no. 5, pp. 97–108. URL: jstor.org/stable/20788647 (date assessed: 09.11.2024)

6. Ferguson-Walter K., Fugate S., Mauger J., Major M. Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security - HotSoS ’19. Nashville, Tennessee: ACM Press, 2019, pp. 1–8. DOI: doi.org/10.1145/3314058.3314063

7. Shade T., Rogers A., Ferguson-Walter K., Elsen S. B., Fayette D., Heckman K. Hawaii International Conference on System Sciences, 2020. URL: pdfs.semanticscholar.org/4f80/8f74597b214bc39a79616c2ab564fd629f55.pdf (дата обращения: 10.11.2024)

8. Kolomojcev V.S.. Postroenie jeshelonirovannyh sistem zashhity informacii. Pervaja Vserossijskaja nauchnaja konferencija. [Building layered information security systems]. Sankt-Peterburg, 2020. pp. 190-192, DOI: doi.org/10.31799/978-5-8088-1452-3-2020-1-190-192, -EDN: YOXMVF

9. Javadpour Amir, Ja'fari Forough, Taleb Tarik Computers & Security, Volume 140, 2024. DOI: doi.org/10.1016/j.cose.2024.103792

10. Jorquera J.M. Handbook of Research on Intrusion Detection Systems, 2020, pp. 105-129, DOI: dx.doi.org/10.4018/978-1-7998-2242-4

11. Javadpour A. Cluster Computing, Volume 26, Issue 1, February 2023, Pages 367-384 Volume 26, Issue 1, February 2023, pp. 367-384 DOI: doi.org/10.1007/s10586-022-03621-3

12. Almeshekah M.H., Spafford E.H. Cyber Deception, Springer, 2016, pp. 25-52 DOI: doi.org/10.1007/978-3-319-32699-3_2

13. Ross R., Pillitteri V., Graubart R., Bodeau D., McQuaid R. National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep. NIST SP 800-160v2, Nov. 2019. DOI: doi.org/10.6028/NIST.SP.800-160v2r1

14. Anwar A.H., Kamhoua C.A. IEEE Transactions on Network and Service Management Volume 19, Issue 3, 2022, pp. 3438-3452. DOI: doi.org/10.1109/TNSM.2022.3179965

15. Javadpour A., Taleb T., Ja'Fari F. Computers & Security, Volume 140, 2024, №103792, DOI: doi.org/10.1016/j.cose.2024.103792

16. Onyekware U. Journal of Information Security, 2021, pp.250-269. DOI: doi.org/10.4236/jis.2021.124014

17. Salimova H.R. Central Asian Research Journal for Interdisciplinary Studies, Volume 2, Issue 5, 2022, pp. 479-486. URL: researchgate.net/publication/221260586_A_Virtual_Honeypot_Framework

18. Spitzner L. Boston: Addison-Wesley Professional, Sep. 2002. URL: theswissbay.ch/pdf/Gentoomen%20Library/Security/0321108957.Addison-Wesley%20Professional.Honeypots-%20Tracking%20Hackers.pdf

19. DejaVU - Open Source Deception Platform. URL: github.com/bhdresh/Dejavu

20. Konkin Ju.V. VII Mezhdunarodnyj nauchno-tehnicheskij forum STNO-2024. Sbornik trudov. Tom 3, pp. 167-171. EDN: UZZJOA.

21. Ayeni O., Alese B., Omotosho L. International Journal of Computer Applications., Volume 70, 2013, №20. DOI: dx.doi.org/10.5120/12197-8136

22. Spitzner Lance Security Focus information, Jan. 2004. DOI: dx.doi.org/10.1109/CSAC.2003.1254322

23. Pawlick J., Colbert E., Zhu Q. ACM Computing Surveys, Volume 52, Issue 4, 2019. DOI: doi.org/10.1145/3337772

24. Crouse M., Prosser B. 2nd MTD@CCS conference, 2015, pp. 21-29. DOI: doi.org/10.1145/2808475.2808480

25. Kak budto mjodom namazano: chto takoe Honeypot i kak pojmat' hakera «na zhivca» [As if smeared with honey: what is a Honeypot and how to catch a hacker "live bait"]. URL: securitylab.ru/analytics/536141.php

26. Bringer M.L., Chelmecki C.A International Journal of Computer Network and Information Security, Volume 4, 2012, № 10, p. 63. DOI: dx.doi.org/10.5815/ijcnis.2012.10.07

27. Scottberg B., Yurcik W., and Doss D. IEEE International Symposium on Technology and Society (ISTAS'02). Raleigh, NC, USA: IEEE, 2002, pp. 387–391. DOI: dx.doi.org/10.1109/ISTAS.2002.1013842

28. Liu G., Ou X., Singhal A., Tabari A.Z. 19ep IFIP International Conference on Digital Forensics, 2023, pp. 73-90. DOI: dx.doi.org/10.1007/978-3-031-42991-0_5

29. Doubleday H. International Journal of Advanced Computer Science and Applications, Vol. 7, No. 5, 2016, pp. 117-121. DOI: dx.doi.org/10.14569/IJACSA.2016.070518

30. Gibbens M., Rajendran H. The University of Arizona, 2012, p. 1-12. URL: cs.arizona.edu/~collberg/Teaching/466566/2013/Resources/presentations/2012/topic12-final/slides.pdf

31. Ochiai H. Honeyboost: Expert Systems with Applications, Volume 201, 1 September 2022, № 117073. DOI: doi.org/10.1016/j.eswa.2022.117073

32. Bilinski M., Gabrys R. 9th International Conference on Decision and Game Theory for Security, Volume 11199 LNCS, 2018, pp. 115-126. DOI: dx.doi.org/10.1007/978-3-030-01554-1_7

33. Ja'fari F. Journal of Ambient Intelligence and Humanized Computing, Volume 12, Issue 2, 2021, pp. 2993-3016. DOI: dx.doi.org/10.1007/s12652-020-02461-6

34. Juels A, Rivest R. L. Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security - CCS '13. Berlin, Germany: ACM Press, 2013, pp. 145–160. DOI: doi.org/10.1145/2508859.2516671

35. Pedersen J.M., Srinivasa S. 38th Annual Computer Security Applications Conference, 2022, pp. 742-755. DOI: doi.org/10.1145/3564625.3564645

36. Bercovitch M., Renford M., Hasson L., Shabtai A., Rokach L. Proceedings of 2011 IEEE International Conference on Intelligence and Security Informatics, Jul. 2011, pp. 131–136. DOI: dx.doi.org/10.1109/ISI.2011.5984063

37. Neal C. 16th International Conference on Network and System Security, 2022, pp. 155-169. DOI: dx.doi.org/10.1007/978-3-031-23020-2_9

38. Yuan J., Yang H., Kong Y. Future Internet, Volume 15, 2023, № 4, p. 127. DOI: doi.org/10.3390/fi15040127

39. Padayachee K. IET Information Security, vol. 9, no. 4, 2014, pp. 240–247. DOI: doi.org/10.1049/iet-ifs.2014.0063

40. Voris J., Jermyn J., Keromytis A. D., Stolfo S. J. B Proceedings of the Cyber Infrastructure Protection Conference, Strategic Studies Institute, 2013, p. 25.DOI: doi.org/10.7916/D8RN3H9S

41. Whitham B. IEEE computer society, 2017. DOI: doi.org/10.24251/HICSS.2017.733

42. Lim C., Budiarto E., Hobert K. 1st IEEE International Conference on Cryptography, Informatics, and Cybersecurity, 2023, pp. 139-144. DOI: doi.org/10.1109/ICoCICs58778.2023.10276639

43. Yamin M.M., Katt B. Computers & Security, Volume 122, 2022, № 102892, DOI: doi.org/10.1016/j.cose.2022.102892

44. Lee J., Choi J., Lee G., Shim S-W., Kim T. Phantom IEEE Access, vol. 8, 2020, pp. 32 203–32 214. DOI: dx.doi.org/10.1109/ACCESS.2020.2973700

45. Sokolovskij S.P. Informatika: problemy, metodologija, tehnologii, Sbornik materialov XIX mezhdunarodnoj nauchno-metodicheskoj konferencii, 2019, pp.639-643.EDN: ZFDMBF

46. Liu G., Ou X., Singhal A., Tabari A.Z. 19ep IFIP International Conference on Digital Forensics, 2023, p. 73-90 DOI: dx.doi.org/10.1007/978-3-031-42991-0_5

47. Zubaida R. Computers & Security, Volume 139, 2024. DOI: doi.org/10.1016/j.cose.2023.103685

48. Vitor A. Pervasive and Mobile Computing Volume 74, 2021. DOI: doi.org/10.1016/j.pmcj.2021.101412

49. Wei D. Information Sciences, Volume 690, 2024. DOI: doi.org/10.1016/j.ins.2024.121554

50. Li L., Just J. Annual Computer Security Applications Conference (ACSAC'06), 2006, pp. 329–338. DOI: doi.org/10.1109/ACSAC.2006.10

51. Zhang Li, Thing L. Computers & Security, Volume 106, 2021, №102288, DOI: doi.org/10.1016/j.cose.2021.102288

52. Okhravi H., Comella A. International Conference on Critical Infrastructure Protection, Advances in Information and Communication Technology, 2011, pp. 107–123. DOI: doi.org/10.1016/j.ijcip.2012.01.002

53. Carlo A. International Journal of Critical Infrastructure Protection, 2024 DOI: doi.org/10.1016/j.ijcip.2024.100701

54. Eng S., How K.C., Zhu Y. Conference on Science, Engineering and Technology, 2023, pp. 587-598. URL: link.springer.com/chapter/10.1007/978-981-19-7222-5_44

55. Larsen P., Homescu A., Brunthaler S., Franz M. Symposium on Security and Privacy, 2014, pp. 276–291. DOI: dx.doi.org/10.1109/SP.2014.25

56. Kang K.W. KSII transactions on internet and information systems, 2022, pp. 1063-1075. URL: syscore.sejong.ac.kr/~woongbak/publications/J38.pdf

57. Putjato M.M., Makarjan A.S., Chich Sh. M., Markova V.K. Prikaspijskij zhurnal: upravlenie i vysokie tehnologii, 2020, № 4 (52), EDN: QXGGTW. DOI: doi.org/10.21672/2074-1707.2020.52.4.085-098

58. Tihonov A.M. Izvestija Instituta Inzhenernoj Fiziki, 2024, №3, pp. 65-71 EDN: QSVNKO

59. Alissa K., Alqahtani M., Faiz T., Alyas T. Mobile Information Systems, 2022, pp. 1-13. DOI: doi.org/10.1155/2022/2600712.

Дата поступления: 17.10.2024

Дата публикации: 30.11.2024