Аннотация. В документе представлен всесторонний анализ публикации, в которой подробно описаны известные тактики, методы и процедуры (TTP), используемые кибер-профессионалами для получения первоначального доступа к облачным системам. Анализ охватывает различные аспекты, включая выявление и использование уязвимостей, различные методы использования облачных технологий, развёртывание специального вредоносного ПО.

Представлены ключевые моменты и полезная информация, которую могут использовать ИБ и ИТ специалисты и специалисты в различных отраслях для улучшения своих защитных стратегий, против спонсируемых государством киберугроз. Понимая адаптированную тактику субъекта для первоначального доступа к облаку, заинтересованные стороны могут лучше предвидеть и снижать потенциальные риски для своей облачной инфраструктуры, тем самым укрепляя свою общую безопасность.

I. Введение

Документ под названием «cyber actors adapt tactics for initial cloud access», опубликованный Агентством национальной безопасности (АНБ) предупреждает, об адаптации тактики для получения первоначального доступа к облачным сервисам, а не для использования уязвимостей локальной сети.

Переход от локальных решений к облачным является ответом на то, что организации модернизируют свои системы и переходят на облачную инфраструктуру. Также кибер-кампании расширяются в сторону таких секторов, как авиация, образование, секторов, связанных региональными и федеральными, а также госучреждениями, правительственными финансовыми департаментами и военными организациями.

Реальность такова, что для взлома облачных сетей нужно только пройти аутентификацию у поставщика облачных услуг, и в случае успеха, защита будет преодолена. Другими словами, «неожиданный» аспект облачных сред: меньшая уязвимость сети по сравнению с локальными системами парадоксальным образом делает преодоление первоначального доступа наиболее эффективным.

За последний год наблюдаемые TTPs были простыми, и вместе с тем эффективными так как использовались служебные и бездействующие учётные записи. В целом публикация вызывает прохладное утешение, предполагая, что прочная основа основ безопасности всего лишь гонка на опережение специалистов по безопасности с атакующими.

II. Ключевые выводы

- **Адаптация к облачным сервисам:** сместился фокус с эксплуатации уязвимостей локальной сети на прямое воздействие на облачные сервисы. Это изменение является ответом на модернизацию систем и миграцию инфраструктуры в облако.
- **Аутентификация как ключевой шаг**: чтобы скомпрометировать облачные сети, необходимо успешно пройти аутентификацию у поставщика облачных услуг. Предотвращение этого первоначального доступа имеет решающее значение для предотвращения компрометации.
- **Расширение таргетинга:** расширена сфера воздействия на сектора, такие как, как авиация, образование, правоохранительные органы, региональные и федеральные организации, правительственные финансовые департаменты и военные организации. Это расширение указывает на стратегическую диверсификацию целей сбора разведывательной информации.
- **Использование служебных и неактивных учётных записей:** подчёркивается, что за последние 12 месяцев использовались брутфорс-атаки для доступа к служебным и неактивным учётным записям. Эта тактика позволяет получить первоначальный доступ к облачным средам.
- **Профессиональный уровень атакующих:** выявлена возможность осуществления компрометациии глобальной цепочки поставок, как, например, инцидент с SolarWinds в 2020 году.
- **Первая линия защиты:** подчёркивается, что первая линия защиты включает предотвращения возможности первичного доступа к сервисам.

III. Адаптация к облачным сервисам

Адаптация атак к облачным сервисам знаменует собой эволюцию в сфере кибершпионажа и кибервойны и представляет собой более глубокую стратегическую адаптацию к меняющейся технологической среде и растущей зависимости правительств и корпораций от облачной инфраструктуры. Переход организаций к облачным сервисам обусловлен преимуществами масштабируемости, экономической эффективности и возможности быстрого развёртывания и обновления

сервисов. Однако этот переход также создаёт новые уязвимости и проблемы для кибербезопасности.

A. *Стратегический переход к облаку*

По мере того, как организации модернизировали свои системы и переходили на облачную инфраструктуру, участники адаптировали свои тактики, методы и процедуры (TTP) к новой среде. Эта адаптация обусловлена осознанием того, что облачные сервисы, централизуя огромные объёмы данных и ресурсов, представляют собой выгодную цель для шпионажа и сбора разведывательной информации. Облачная архитектура, предлагая организациям многочисленные преимущества, также требует переоценки стратегий безопасности для устранения уникальных уязвимостей.

B. *Тактика, методы и процедуры (TTP)*

Адаптация участников к облачным сервисам включает в себя ряд сложных TTP, предназначенных для использования конкретных характеристик облачных сред. Один из основных методов получения первоначального доступа к облачным сетям включает аутентификацию у поставщика облачных услуг, что достигается различными способами, включая подбор пароля и password-spray для доступа к служебным и неактивным учётным записям. Эти учётные записи, часто используемые для запуска приложений и управления ими без прямого контроля со стороны человека, особенно уязвимы, поскольку они могут быть не защищены многофакторной аутентификацией (MFA) и обладать высокими уровнями привилегий.

Кроме того, было замечено, что использование для аутентификации выданных системой токенов позволяет убрать необходимость в паролях. Дополнительно использовался процесс регистрации новых устройств в облаке с обходом механизмов безопасности MFA, в частности, с помощью таких методов, как «бомбардировка MFA», с целью случайного одобрения пользователем одного из этих запросов как легитимного. Кроме того, использование резидентных прокси-серверов для сокрытия своего присутствия в Интернете и затруднения обнаружения вредоносной деятельности представляет собой ещё один уровень профессионального подхода.

C. *Последствия*

Адаптация участников к целевым облачным сервисам имеет серьёзные последствия для кибербезопасности. Это подчёркивает необходимость внедрения надёжных мер безопасности, адаптированных к облачной среде. Сюда входит применение политик надёжных паролей, внедрение MFA, управление и мониторинг служебных и неактивных учётных записей, а также настройка политик регистрации устройств для предотвращения несанкционированного доступа. Кроме того, корректировка срока действия токенов, выпущенных системой, и использование средств защиты на уровне сети для обнаружения и предотвращения использования резидентных прокси-серверов являются важными шагами в защите от этих угроз.

IV. Детали TTP:

- **Доступ к учётным данным / подбор пароля T1110**: используются password-spray и подбор паролей в качестве начальных векторов заражения. Подход предполагает попытку ввода нескольких паролей для разных учётных записей или многочисленные попытки для одной учётной записи для получения несанкционированного доступа.
- **Первоначальный доступ / T1078.004 Действительные учётные записи: Облачные учётные записи:** получение доступа к облачным сервисам, используя скомпрометированные учётные данные: как системные учётные записи (используемые для автоматизированных задач и служб), так и неактивные учётные записи, учётные которые все ещё остаются в системе.
- **Доступ к учётным данным / T1528 Кража токена доступа к приложению:** злоумышленники используют украденные токены доступа для входа в учётные записи без необходимости ввода паролей. Токены доступа — это цифровые ключи, которые позволяют получить доступ к учётным записям пользователей. Их получение позволяет обойти традиционные механизмы входа в систему.
- **Доступ к учётным данным / Формирование запроса многофакторной аутентификации T1621:** метод «бомбардировка MFA» предполагает, что злоумышленники неоднократно отправляют запросы MFA на устройство жертвы. Цель состоит в том, чтобы жертва приняла запрос и таким образом предоставила злоумышленнику доступ.
- **Командование и контроль / T1090.002 Прокси: Внешний прокси:** чтобы поддерживать «тайные операции и сливаться с обычным трафиком», используются открытые прокси, расположенные в частных диапазонах IP-адресов, т.к. вредоносные соединения сложнее отличить от легальной активности пользователей в журналах доступа.
- **Постоянство / T1098.005 Манипулирование учётными записями: Регистрация устройств:** после получения доступа к учётным записям предпринимаются попытки зарегистрировать свои собственные устройства в облачном клиенте. Успешная регистрация устройства может обеспечить постоянный доступ к облачной среде.

A. *Доступ через сервисные и спящие учётные записи*

Одна из ключевых стратегий, применяемых злоумышленниками, предполагает нацеливание на сервисные и неактивные учётные записи в облачных средах. Учётные записи служб используются для запуска приложений и служб и управления ими без прямого взаимодействия с человеком. Эти учётные записи особенно уязвимы, поскольку их часто невозможно защитить с помощью многофакторной аутентификации (MFA), и они могут иметь высокопривилегированный доступ в зависимости от их роли в управлении приложениями и

службами. Получив доступ к этим учётным записям, злоумышленники могут получить привилегированный первоначальный доступ к сети, которую они используют в качестве стартовой площадки для дальнейших операций.

Кампании нацелены на неактивные учётные записи, пользователи которых больше не активны в организации-жертве, но не были удалены из системы. Эти учётные записи могут быть использованы для восстановления доступа к сети, особенно после мер реагирования на инциденты, таких как принудительный сброс пароля. Было замечено, что субъекты входили в эти неактивные учётные записи и следовали инструкциям по сбросу пароля, что позволяло им сохранять доступ даже после того, как группы реагирования на инциденты пытались их «выселить».

B. Аутентификация токена на основе облака

Ещё один TTP — это использование аутентификации на основе облачных токенов. Замечено, что злоумышленники использовали выданные системой токены доступа для аутентификации в учётных записях жертв без необходимости ввода пароля. Этот метод позволяет обходить традиционные методы аутентификации на основе учётных данных и может быть особенно эффективным, если срок действия этих токенов длительный, или если токены не защищены должным образом.

C. Брутфорс и password-spray

Использование злоумышленниками атаки (T1110) применяется в качестве начальных векторов заражения. Метод включают попытку доступа к учётным записям путём перебора множества паролей или использования общих паролей для многих учётных записей соответственно. Метод часто бывает успешен из-за использования слабых или повторно используемых паролей для разных учётных записей.

D. Роль токенов доступа

Токены доступа являются неотъемлемой частью современных систем аутентификации, особенно в облачных средах. Они предназначены для упрощения процесса входа в систему для пользователей и обеспечения безопасного метода доступа к ресурсам без повторного ввода учётных данных. Токены выдаются после того, как пользователь входит в систему с именем и паролем, и их можно использовать для последующих запросов аутентификации.

E. Риски, связанные с аутентификацией токенов

Хотя аутентификация на основе токенов может обеспечить удобство и безопасность, она также создаёт определённые риски, если ею не управлять должным образом. Если злоумышленники получат эти токены, они смогут получить доступ к учётным записям без необходимости знания пароли, особенно если токены имеют длительный срок действия.

F. Настройка срока действия токена

Отмечается, что время действия токенов, выпущенных системой, по умолчанию может варьироваться в зависимости от используемой системы. Однако для облачных платформ крайне важно предоставить администраторам возможность регулировать время действия этих токенов в соответствии с их потребностями в безопасности. Сокращение срока действия токенов может уменьшить окно возможностей для несанкционированного доступа, если токены будут скомпрометированы.

G. Обход аутентификации по паролю и MFA

Отмечается, что обход аутентификации по паролю в учётных записях с помощью повторного использования учётных данных и password-spray. Метод предполагает попытку получить доступ к большому количеству учётных записей с использованием часто используемых паролей, в то время как повторное использование учётных данных позволяет пользователям повторно использовать одни и те же пароли для нескольких учётных записей

Также применяется техника «бомбардировка MFA» (T1621), для обхода систем MFA. Метод предполагает повторную отправку запросов MFA на устройство жертвы до тех пор, пока жертва, перегруженная постоянными уведомлениями, не примет запрос. Метод эффективно использует человеческую психологию и неудобство повторных уведомлений для обхода надёжных мер безопасности.

H. Регистрация новых устройств в облаке

После преодоления первоначальных барьеров выполняется регистрация собственных устройств в качестве новых (T1098.005). Этот шаг имеет решающее значение для сохранения доступа к облачной среде и облегчения дальнейших вредоносных действий. Успех тактики зависит от отсутствия строгих правил проверки устройств в конфигурации безопасности арендатора облака. Без надлежащих мер проверки устройств крайне легко добавить неавторизованные устройства в сеть, предоставив им доступ к конфиденциальным данным и системам.

I. Защита от несанкционированной регистрации устройств

Внедряя строгие правила проверки устройств и политики регистрации, организации могут значительно снизить риск несанкционированной регистрации устройств. Известны случаи, когда эти меры были эффективно применены, успешно защитили от злоумышленников, лишив их доступа к арендатору облака.

J. Резидентные прокси и их использование

Резидентные прокси — это промежуточные службы, которые позволяют пользователям маршрутизировать трафик через IP-адрес, предоставленный интернет-провайдером (ISP), который обычно присваивается резидентному адресу. Из-за этого трафик выглядит так, как будто он исходит от обычного пользователя, что может быть особенно полезно для целей слиться с обычным трафиком и избежать раскрытия.

Использование резидентных прокси-серверов служит целью сокрытия истинного местонахождения и источника их вредоносной деятельности. Создавая впечатление, что их трафик исходит из диапазонов легитмных провайдеров. Тактика усложняет обеспечение безопасности, которые полагаются на репутацию IP-адреса или геолокацию как на индикаторы компрометации.

K. *Проблемы, создаваемые резидентными прокси*

Эффективность резидентных прокси-серверов в сокрытии источника трафика представляет собой проблему для сетевой защиты. Традиционные меры безопасности, которые отслеживают и блокируют известные вредоносные IP-адреса, неэффективны против использующих резидентные прокси-серверы, поскольку эти IP-адреса могут не иметь предыстории вредоносной активности и неотличимы от IP-адресов законных пользователей.

V. Аутентификация как ключевой шаг

A. *Аутентификация как ключевой шаг в облачной безопасности*

В изменяющемся кибер-ландшафте адаптация к целевым облачным сервисам подчёркивает кардинальный сдвиг в тактике кибершпионажа. Переход от использования уязвимостей локальной сети к прямому нацеливанию на облачные инфраструктуры знаменует собой значительную эволюцию киберугроз. В основе этого лежит решающая роль аутентификации как ключевого шага в защите облачных сетей от кибер-профессионалов.

B. *Важность аутентификации в облачных средах*

Аутентификация служит шлюзом к облачным сервисам, определяя, следует ли предоставить доступ пользователю или системе. В облачных средах, где ресурсы и данные размещаются за пределами предприятия и доступны через Интернет, невозможно переоценить важность надёжных механизмов аутентификации. В отличие от традиционных локальных систем, где есть меры физической безопасности и внутренняя сетевая защита, облачные сервисы по своей сути более подвержены воздействию Интернета. Такая уязвимость делает начальный этап аутентификации не просто мерой безопасности, а критически важным механизмом защиты от несанкционированного доступа.

C. *Проблемы облачной аутентификации*

Переход к облачным сервисам приносит с собой уникальные проблемы в реализации эффективных стратегий аутентификации. Пользователи получают доступ к облачным сервисам из разных мест, устройств и сетей, что требует эффективных механизмов аутентификации.

Масштабируемость облачных сервисов означает, что механизмы аутентификации должны быть в состоянии обрабатывать большое количество запросов на доступ без значительных задержек и ухудшения пользовательского опыта. Это требование масштабируемости и удобства для пользователя часто противоречит необходимости строгих мер безопасности, создавая хрупкий баланс, который должны соблюдать организации.

D. *Стратегии усиления облачной аутентификации*

- **Многофакторная аутентификация (MFA).** MFA добавляет дополнительный уровень безопасности, требуя от пользователей предоставления двух или более факторов проверки для получения доступа. Подход снижает риск несанкционированного доступа, поскольку значительно сложнее получить несколько факторов аутентификации.
- **Адаптивная аутентификация.** Механизмы адаптивной аутентификации корректируют требования в зависимости от контекста запроса доступа. Такие факторы, как местоположение, устройство и поведение пользователя, могут влиять на процесс аутентификации, что позволяет применять более строгий контроль в сценариях повышенного риска.
- **Архитектура нулевого доверия.** Принятие подхода нулевого доверия к облачной безопасности, при котором ни один пользователь или система не пользуется доверием по умолчанию, может повысить эффективность аутентификации. Эта модель требует строгой проверки личности каждого кто пытается получить доступ к ресурсам, независимо от их местоположения или сети.
- **Использование биометрии.** Методы биометрической аутентификации, такие как сканирование отпечатков пальцев или распознавание лиц, обеспечивают высокий уровень безопасности за счёт использования уникальных физических характеристик пользователей. Эти методы могут быть особенно эффективными для предотвращения несанкционированного доступа в облачных средах.
- **Шифрование данных аутентификации.** Шифрование данных аутентификации (паролей, токенов аутентификации и другой конфиденциальной информации), как при передаче, так и при хранении, может защитить от перехвата и использования злоумышленниками.

VI. Первоначальный доступ

A. *Возросшая важность первоначального доступа в облачной безопасности*

Смещение акцента кибер-профессионалов на облачные сервисы вывело важность обеспечения первоначального доступа на передний план. В облачных средах первоначальный доступ представляет собой критический момент, когда безопасность всей системы становится наиболее уязвимой. В отличие от традиционных локальных сетей, доступ к облачным сервисам осуществляется через Интернет, что делает начальную точку входа основной целью для злоумышленников.

B. *Первоначальный доступ как плацдарм для злоумышленников*

Получение первоначального доступа к облачным сервисам позволяет злоумышленникам закрепиться в целевой среде с последующим повышением привилегий, распространения по сети и получения доступа к конфиденциальным данным. Распределённый характер облачных сервисов также означает, что компрометация одной учётной записи может потенциально предоставить доступ к широкому спектру ресурсов и данных.

C. *Проблемы в обеспечении первоначального доступа*

- **Удалённый доступ.** Облачные сервисы предназначены для удалённого доступа, что увеличивает поверхность атаки.
- **Управление идентификацией и доступом (IAM).** В облачных средах IAM становится важнейшим компонентом безопасности. Организации должны обеспечить надёжность политик IAM и предоставление разрешений на основе принципа наименьших привилегий, чтобы минимизировать риск первоначального доступа со стороны неавторизованных лиц.
- **Фишинг и социнженерия.** используются методы фишинга и социальной инженерии для получения первоначального доступа. Эти методы используют человеческий фактор, а не технические уязвимости, что затрудняет защиту от них с помощью традиционных мер безопасности.

D. *Примеры методов первоначального доступа*

- **Credential Stuffing.** Метод предполагает использование ранее взломанных пар имени пользователя и пароля для получения несанкционированного доступа к учётным записям, делая ставку на вероятность того, что люди будут повторно использовать учётные данные в нескольких службах.
- **Использование некорректных конфигураций.** Облачные сервисы сложно настроить правильно, и используются некорректные конфигурации: открытые сетевые сегменты или ошибки в настройке управления доступом.
- **Компрометация сторонних сервисов.** Злоумышленники могут атаковать сторонние сервисы, которые интегрируются с облачными средами, например приложения SaaS, чтобы получить первоначальный доступ к облачной инфраструктуре.

E. *Снижение рисков первоначального доступа*

- **Комплексные политики доступа.** Установление и соблюдение комплексных политик доступа может помочь контролировать, кто и на каких условиях имеет доступ к облачным ресурсам.
- **Регулярные аудиты и проверки.** Проведение регулярных аудитов и проверок журналов доступа и разрешений может помочь выявить и устранить потенциальные уязвимости до того, как они будут использованы.
- **Обучение по вопросам безопасности.** Обучение сотрудников рискам фишинга и социальной инженерии может снизить вероятность компрометации учётных данных.
- **Endpoint Security.** Обеспечение безопасности и актуальности всех устройств с доступом к облачным сервисам, может помешать злоумышленникам использовать уязвимости конечных точек для получения первоначального доступа.
- **Обнаружение аномалий.** Внедрение систем обнаружения аномалий помогает выявить необычные модели доступа или попытки входа в систему, которые могут указывать на попытку взлома.

VII. Расширение сферы деятельности

A. *Расширение таргетинга*

Стратегическое расширение деятельности на более широкий круг секторов является тревожным событием в сфере глобальной безопасности. Такая диверсификация целей отражает расчётливый подход к использованию взаимосвязанного характера современных отраслей и растущей зависимости от облачных сервисов в различных секторах.

B. *Расширение сферы шпионажа*

Расширение таких секторов, как авиация, образование, правоохранительные органы, местные и федеральные учреждения, правительственные финансовые ведомства и военные организации, демонстрирует их намерение собирать разведданные из широкого спектра источников. Широкая стратегия таргетинга предполагает, что они заинтересованы не только в традиционной информации, связанной с национальной безопасностью, но также в получении разнообразного набора данных, которые могут обеспечить экономические, политические или технологические преимущества.

C. *Последствия для различных секторов*

- **Авиация.** Авиационная отрасль включает в себя сложную экосистему авиакомпаний, аэропортов, производителей и служб поддержки, каждая из которых обрабатывает конфиденциальные данные, связанные с национальной безопасностью и запатентованными технологиями.
- **Образование.** Университеты и исследовательские институты являются источниками передовых исследований и интеллектуальной собственности. Их часто таргетируют за новаторскую работу в области науки, технологий и обороны.
- **Правоохранительные органы.** организации хранят конфиденциальные данные об уголовных расследованиях, вопросах национальной безопасности и личную информацию граждан, что делает их ценной целью для шпионажа.
- **Местные и федеральные учреждения.** Органы местного и федерального самоуправления управляют критически важной инфраструктурой, госуслугами и имеют доступ к огромным объёмам персональных данных, которые могут быть использованы для различных злонамеренных целей.
- **Государственные финансовые департаменты.** департаменты обрабатывают конфиденциальные экономические данные и имеют представление о

национальных финансовых стратегиях и политике, что может быть ценным для иностранных разведывательных служб.

- **Военные организации.** представляют большой интерес из-за их стратегической важности и доступа к секретной информации об оборонных возможностях, операциях и технологиях.

D. Проблемы защиты широкого круга целей

- **Разнообразие подходов к обеспечению безопасности.** Разные отрасли имеют разные уровни зрелости и ресурсов кибербезопасности, что делает некоторые из них более уязвимыми для сложных киберугроз.
- **Взаимосвязь.** Взаимосвязанный характер этих секторов означает, что нарушение в одной области может иметь каскадные последствия для других, как это видно в атаках на цепочки поставок.

E. Стратегии снижения рисков

- **Секторальные механизмы кибербезопасности.** Разработка и внедрение механизмов кибербезопасности, адаптированных к уникальным потребностям и рискам каждого сектора, может повысить общую безопасность.
- **Обмен информацией.** Обмен информацией об угрозах и лучшими практиками внутри секторов и между ними может помочь организациям опережать возникающие угрозы и координировать реагирование на инциденты.
- **Регулярные оценки безопасности.** Проведение регулярных оценок безопасности и тестирования на проникновение может помочь организациям выявлять и устранять уязвимости до того, как они будут использованы.
- **Безопасность цепочки поставок.** Укрепление безопасности цепочки поставок имеет решающее значение, поскольку злоумышленники часто нацелены на менее защищённые элементы в цепочке поставок, чтобы получить доступ к более крупным организациям.
- **Планирование реагирования на инциденты.** Наличие чётко определённого плана реагирования на инциденты может гарантировать, что организации готовы быстро и эффективно реагировать на нарушения.

VIII. Использование Сервисных и неактивных учётных записей

A. Использование сервисных и неактивных учётных записей в кибератаках

Эксплуатация сервисных и неактивных учётных записей кибер-профессионалами представляет собой изощренный и часто упускаемый из виду вектор кибератак. Эти учётные записи, созданные для различных операционных целей в облачных и локальных средах организации, могут предоставить злоумышленникам доступ, необходимый им для достижения своих целей, если они не управляются и не защищаются должным образом.

B. Понимание сервисных и неактивных учётных записей

Учётные записи служб — это специализированные учётные записи, используемые приложениями или службами для взаимодействия с операционной системой или другими службами. Они часто имеют повышенные привилегии для выполнения определённых задач и могут не быть привязаны к личности отдельного пользователя. С другой стороны, неактивные учётные записи — это учётные записи пользователей, которые больше не используются либо потому, что пользователь покинул организацию, либо потому, что цель учётной записи была достигнута. Эти учётные записи особенно опасны, поскольку о них часто забывают, им оставляют больше привилегий, чем необходимо, и они не контролируются так тщательно, как активные учётные записи пользователей.

C. Почему служебные и неактивные учётные записи подвергаются атаке

- **Повышенные привилегии.** Учётные записи служб имеют повышенные привилегии, необходимые для системных задач, которые можно использовать для получения широкого доступа к сети организации.
- **Отсутствие мониторинга.** Неактивные учётные записи используются нерегулярно, что снижает вероятность их отслеживания на предмет подозрительной активности делает их привлекательной целью для злоумышленников.
- **Слабые учётные данные или учётные данные по умолчанию.** Учётные записи служб могут быть настроены со слабыми учётными данными или учётными данными по умолчанию, которые проще найти с помощью атак методом перебора.
- **Обход аналитики поведения пользователей.** Поскольку учётные записи служб выполняют автоматизированные задачи, их модели поведения могут быть предсказуемыми, что позволяет вредоносным действиям сливаться с обычными операциями и уклоняться от обнаружения.

D. Угроза, которую представляют скомпрометированные учётные записи

- **Распространение:** использование привилегий учётной записи для дальнейшего распространения в сети, получая доступ к другим системам и данным.
- **Повышение привилегий:** использование учётной записи для повышения привилегий и получения административного доступа к критически важным системам.
- **Закрепление:** обеспечение постоянного присутствия в сети, что затрудняет обнаружение и устранение злоумышленника.
- **Эксфильтрация данных:** доступ к конфиденциальным данным и их удаление, что

приводит к утечке данных и краже интеллектуальной собственности.

E. Снижение рисков, связанных с сервисными и неактивными счетами

- **Регулярные проверки.** Проведение регулярных проверок всех учётных записей для выявления и деактивации неактивных учётных записей и обеспечения того, чтобы учётные записи служб имели минимально необходимые привилегии.
- **Строгий контроль аутентификации.** Применение политики надёжных паролей и использование MFA для учётных записей служб, где это возможно.
- **Мониторинг.** Внедрение механизмов мониторинга и оповещения для обнаружения необычных действий, связанных со службами и неактивными учётными записями.
- **Разделение ролей.** Применение принципа разделения ролей к учётным записям служб, чтобы ограничить объем доступа и снизить риск неправомерного использования.
- **Инструменты автоматического управления.** Использование инструментов автоматического управления учётными записями, чтобы отслеживать использование и жизненный цикл учётной записи, гарантируя, что учётные записи будут деактивированы, когда они больше не нужны.

IX. Изощрённость атак

A. Сложность кибероперaций

Отмечался высокий уровень сложности атак, что отражает глубокое понимание киберландшафта и способность адаптироваться в условиях меняющихся мер безопасности. Эта изощрённость очевидна не только в технических возможностях, но и в их стратегическом подходе к кибершпионажу, который включает в себя тщательный выбор целей, планирование и использование передовых тактик, методов и процедур (TTP).

B. Техническое мастерство и инновации

Кибероперации характеризуются использованием специального вредоносного ПО и уязвимостей нулевого дня. Эксплуатация этих уязвимостей позволяет эффективно проникать, например chain-атака SolarWinds, в результате которой был нарушен процесс разработки ПО путём внедрения вредоносного кода в обновление ПО, что затронуло клиентов, включая правительственные учреждения и компании из списка Fortune 500.

C. OpSec и скрытность

OpSec является отличительной чертой операций, и атакующие делают все возможное, чтобы замести следы и сохранить скрытность в скомпрометированных сетях. Это включает в себя использование зашифрованных каналов для кражи данных, тщательное управление серверами управления и контроля во избежание обнаружения, а также использование легитимных инструментов и услуг (LOTL), чтобы гармонировать с обычной сетевой деятельностью. Способность вести себя сдержанно в целевых сетях часто позволяет им проводить долгосрочные шпионские операции без обнаружения.

D. Тактика психологической и социальной инженерии

Помимо технических возможностей, он продемонстрировал искусность в тактике психологической и социальной инженерии. Эти методы предназначены для манипулирования людьми с целью разглашения конфиденциальной информации или выполнения действий, ставящих под угрозу безопасность. Фишинговые кампании, целевой фишинг и другие формы социнженерии часто используются для получения первоначального доступа к целевым сетям или для повышения привилегий внутри них.

E. Выбор цели и сбор разведданных

Процесс выбора цели носит стратегический характер и соответствует национальным интересам России. Цели тщательно выбираются на основе их потенциала предоставления ценной разведывательной информации, будь то политическая, экономическая, технологическая или военная. Как только цель скомпрометирована, участники сосредотачиваются на долгосрочном доступе и сборе разведданных, отдавая предпочтение скрытности и закреплению вместо немедленной выгоды.

F. Адаптируемость к ландшафту кибербезопасности

Одним из наиболее определяющих аспектов является его адаптивность. Переход в сторону облачных сервисов и использования сервисных и неактивных учётных записей является свидетельством такой адаптивности.

G. Базовые механизмы защиты

- **Контроль доступа:** обеспечение того, чтобы только авторизованные пользователи имели доступ к информационным системам и данными чтобы они могли выполнять только те действия, которые необходимы для их роли.
- **Шифрование данных:** защита данных при хранении и передаче посредством шифрования, что делает их нечитаемыми для неавторизованных пользователей.
- **Управление исправлениями:** регулярное обновление программного обеспечения и систем для устранения уязвимостей и снижения риска эксплуатации.
- **Брандмауэры и системы обнаружения вторжений (IDS):** внедрение брандмауэров для блокировки несанкционированного доступа и IDS для мониторинга сетевого трафика на предмет подозрительной активности.
- **Многофакторная аутентификация (MFA):** требование от пользователей предоставления двух или более факторов проверки для получения доступа к системам, что значительно повышает безопасность.
- **Обучение по вопросам безопасности:** обучение сотрудников рискам кибербезопасности и

передовым методам предотвращения атак социальной инженерии и других угроз.

- **Планирование реагирования на инциденты:** подготовка к потенциальным инцидентам безопасности с помощью чётко определённого плана реагирования и восстановления.

H. Роль механизмов в защите от сложных угроз

Многие из кибер-стратегий по-прежнему используют основные недостатки безопасности, такие как плохое управление паролями, необновленное ПО и недостаточный контроль доступа. Придерживаясь базовых механизмов безопасности, организации могут устранить эти уязвимости, значительно усложняя злоумышленникам первоначальный доступ или распространение внутри сети.

Например, реализация MFA может предотвратить несанкционированный доступ, даже если учётные данные скомпрометированы. Регулярное управление исправлениями может закрыть уязвимости до того, как они смогут быть использованы в ходе атаки нулевого дня. Обучение по вопросам безопасности может снизить риск того, что сотрудники станут жертвами фишинга или других тактик социальной инженерии.

I. Проблемы в поддержании механизмов безопасности

Несмотря на очевидные преимущества, поддержание «прочного фундамента безопасности» может оказаться непростой задачей для организаций. Это связано с множеством факторов, включая ограниченность ресурсов, сложность современной ИТ-среды и быстрые темпы технологических изменений. Кроме того, по мере того, как организации все чаще внедряют облачные сервисы и другие передовые технологии, среда становится более сложной, что требует постоянной адаптации фундаментальных методов обеспечения безопасности.

J. Стратегии усиления защиты

- **Непрерывная оценка рисков:** регулярная оценка состояния безопасности организации для выявления уязвимостей и определения приоритетности усилий по их устранению.
- **Использование структур безопасности:** принятие комплексных структур безопасности, таких как NIST Cybersecurity Framework, для руководства внедрением лучших практик и средств контроля.
- **Автоматизация процессов безопасности:** использование автоматизации для оптимизации процессов безопасности, таких как управление исправлениями и мониторинг, для повышения эффективности и результативности.
- **Формирование культуры безопасности:** создание культуры безопасности внутри организации, где кибербезопасность рассматривается как общая ответственность всех сотрудников.
- **Сотрудничество и обмен информацией:** участие в сотрудничестве и обмене информацией с коллегами по отрасли и государственными учреждениями, чтобы оставаться в курсе возникающих угроз и передового опыта.

X. Меры по смягчению последствий

- **Внедрение многофакторную аутентификацию (MFA).** MFA — это один из наиболее эффективных способов защиты учётных записей пользователей от компрометации. Требуя несколько форм проверки, MFA значительно затрудняет злоумышленникам получение несанкционированного доступа, даже если они получили учётные данные пользователя.
- **Регулярная установка исправлений и обновлений.** Поддержание актуальности программного обеспечения и систем с использованием последних исправлений имеет решающее значение для устранения брешей в безопасности, которыми могут воспользоваться злоумышленники. Должен быть установлен регулярный процесс управления исправлениями, чтобы обеспечить своевременное применение обновлений.
- **Сегментация сети.** Разделение сети на более мелкие контролируемые сегменты ограничивает возможность злоумышленника перемещаться внутри сети и получать доступ к конфиденциальным областям. Сегментация также помогает сдерживать потенциальные нарушения в меньшем подмножестве сети.
- **Защита конечных точек.** Развёртывание расширенных решений для защиты конечных точек может помочь обнаружить и предотвратить вредоносные действия на устройствах, имеющих доступ к сети организации. Это включает в себя использование антивирусного программного обеспечения, систем предотвращения вторжений на базе хоста и инструментов обнаружения и реагирования на конечных точках (EDR).
- **Обучение по вопросам безопасности.** Обучение сотрудников рискам и передовым методам кибербезопасности имеет важное значение для предотвращения атак социальной инженерии, таких как фишинг. Регулярное обучение может помочь создать культуру осведомлённости о безопасности внутри организации.
- **Контроль доступа с наименьшими привилегиями.** Обеспечение пользователей только правами доступа, необходимыми для их роли, помогает минимизировать потенциальное воздействие компрометации учётной записи. Средства контроля доступа должны регулярно пересматриваться и корректироваться по мере необходимости.
- **Планирование реагирования на инциденты.** Наличие чётко определённого и проверенного плана реагирования на инциденты позволяет организациям быстро и эффективно реагировать на инциденты безопасности, сводя к минимуму ущерб и восстанавливая операции как можно скорее.
- **Непрерывный мониторинг и обнаружение.** Реализация возможностей непрерывного мониторинга и обнаружения может помочь выявить подозрительные действия на раннем этапе. Сюда

входит использование систем управления информацией о безопасности и событиями (SIEM), систем обнаружения вторжений (IDS) и анализа сетевого трафика.

- **Безопасная конфигурация и усиление защиты.** Системы должны быть надёжно настроены и защищены от атак. Это включает в себя отключение ненужных служб, применение параметров безопасной конфигурации и обеспечение включения функций безопасности.
- **Резервное копирование и восстановление.** Регулярное резервное копирование критически важных данных и систем, а также надёжные процедуры восстановления необходимы для устойчивости к программам-вымогателям и другим разрушительным атакам. Резервные копии следует регулярно проверять, чтобы гарантировать, что на них можно положиться в чрезвычайной ситуации.

A. *Проблемы в реализации мер по смягчению последствий*

Хотя эти меры по смягчению последствий теоретически эффективны, организации часто сталкиваются с проблемами при их реализации. Эти проблемы могут включать ограниченность ресурсов, сложность ИТ-среды, потребность в специализированных навыках и сложность балансировки безопасности с бизнес-требованиями. Кроме того, быстро меняющаяся природа киберугроз означает, что стратегии смягчения их последствий должны постоянно пересматриваться и обновляться.

B. *Совместные усилия и обмен информацией*

Чтобы преодолеть эти проблемы и повысить эффективность мер по смягчению последствий, организации могут участвовать в совместных усилиях и обмене информацией с отраслевыми партнёрами, государственными учреждениями и сообществами кибербезопасности. Такое сотрудничество обеспечивает доступ к общим знаниям, информации об угрозах и передовым практикам, которые могут информировать и улучшать усилия организации по смягчению последствий.

XI. Преимущества и недостатки документа

Документ содержит ценную информацию и рекомендации для организаций по защите от кибер-профессионалов, нацеленных на облачные сервисы. Однако динамичный характер киберугроз и сложность облачных сред означают, что организации должны постоянно обновлять свои методы обеспечения безопасности, а не полагаться исключительно на статические рекомендации.

A. *Преимущества:*

- **Осведомлённость**: документ повышает осведомлённость об изменении тактики в сторону облачных сервисов, что имеет решающее значение для понимания организациями текущего ландшафта угроз.
- **Подробные TTP**: он предоставляет подробную информацию о тактиках, методах и процедурах (TTP), используемых участниками, включая использование сервисных и неактивных учётных записей, что может помочь организациям выявить потенциальные угрозы и уязвимости.
- **Секторальная информация**: описывается расширение охват таких секторов, как авиация, образование, правоохранительные органы и военные организации, предлагая отраслевую информацию, которая может помочь этим отраслям укрепить свою обороноспособность.
- **Стратегии смягчения последствий:** предлагает практические стратегии смягчения последствий, которые организации могут реализовать для усиления своей защиты от первоначального доступа со стороны субъектов, таких как внедрение MFA и управление системными учётными записями.

B. *Недостатки:*

- **Ресурсоёмкость**: реализация рекомендуемых мер по снижению рисков может потребовать значительных ресурсов, что может оказаться затруднительным для небольших организаций с ограниченными бюджетами и персоналом в области кибербезопасности.
- **Сложность облачной безопасности**: в документе указываются проблемы, присущие обеспечению безопасности облачной инфраструктуры, которые могут потребовать специальных знаний и навыков, которыми обладают не все организации.
- **Развивающаяся тактика:** хотя в документе представлены текущие TTП, тактика участников постоянно развивается, а это означает, что защита, основанная исключительно на этих рекомендациях, может быстро устареть.
- **Потенциал чрезмерного акцента на конкретных угрозах:** слишком большое внимание к таким субъектам может привести к тому, что организации пренебрегут другими векторами угроз, которые столь же опасны, но не описаны в документе.
- **Модель общей ответственности:** документ подразумевает модель общей ответственности за облачную безопасность, что может привести к путанице в разделении обязанностей по обеспечению безопасности между поставщиками облачных услуг и клиентами.
- **Ложное чувство безопасности:** у организаций может возникнуть ложное чувство безопасности, полагаясь на предложенные меры по смягчению последствий, не принимая во внимание необходимость динамической и адаптивной системы безопасности для реагирования на новые угрозы.