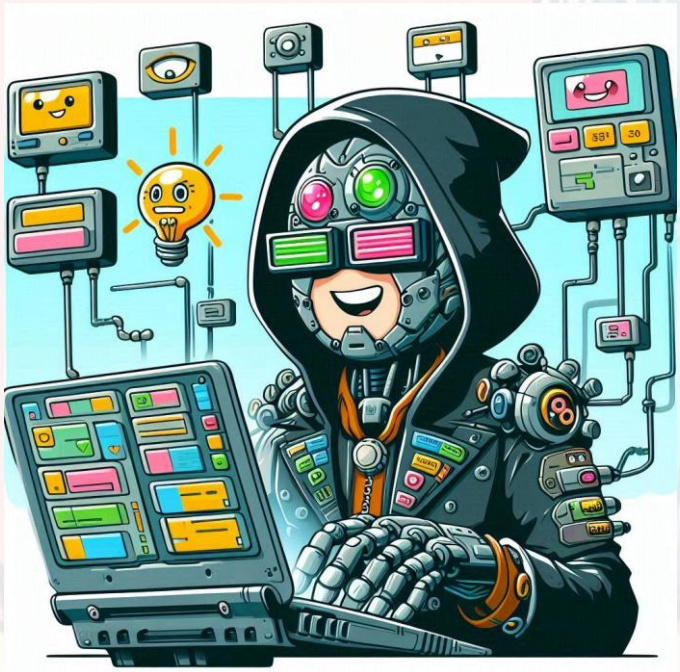

Аннотация – В документе представлен анализ рекомендаций Агентства национальной безопасности (АНБ) по борьбе с LOTL-атаками. Анализ включает в себя изучение подхода к тактике LOTL, подразумевающей использование легитимных инструментов в различных целях.

Анализ предлагает качественное изложение рекомендаций АНБ и служит ценным ресурсом для специалистов по безопасности, ИТ-персонала, политиков и заинтересованных сторон в различных отраслях, предоставляя им знания для защиты от сложных LOTL-угроз.

I. Введение

Документ, озаглавленный "Joint Guidance: Identifying and Mitigating LOTL Techniques", содержит рекомендации о том, как организации могут лучше защитить себя от методов известных как Living Off The Land (LOTL). Эти методы предполагают, что атакующие используют легитимные инструменты и программное обеспечение, присутствующие в среде объекта, для осуществления вредоносных действий, что усложняет обнаружение. Этот подход направлен на сокращение таких легитимных инструментов операционной системы и приложений для нецелевого применения.

Руководство основано на практических результатах, оценках red team, отраслевых практиках и практиках по реагированию на инциденты. Также подчёркивается важность создания и поддержания инфраструктуры, которая собирает и систематизирует данные, помогающие правозащитникам выявлять методы LOTL, адаптированные к ландшафту рисков каждой организации и её ресурсным возможностям.

A. Ключевые моменты

- Руководство составлено крупнейшими агентствами кибербезопасности и национальной безопасности США, Австралии, Канады, Соединённого Королевства и Новой Зеландии и посвящено распространённым методам LOTL и пробелам в возможностях киберзащиты.
- LOTL применяется для компрометации и поддержания доступа к критически важной инфраструктуре, путём использования легитимных системных инструментов и процессов, чтобы «вписаться в обычную активность» и избежать обнаружения.
- Многим организациям трудно обнаружить вредоносную активность LOTL из-за неадекватных методов обеспечения безопасности и управления сетью, отсутствия общепринятых индикаторов компрометации и сложности отличить вредоносную активность от легитимного поведения.
- Рекомендации включают использование детализированного журнала событий, установление базовых показателей активности, использование автоматизации для непрерывного анализа, снижение количества оповещений и использование аналитики поведения пользователей и объектов (UEBA).
- Усиление безопасности включают применение рекомендаций поставщика по усилению безопасности, внедрение списка разрешённых приложений, улучшение сегментации сети и мониторинга, а также усиление контроля аутентификации и авторизации.
- Производителям программного обеспечения рекомендуется применять принципы secure-by-design, чтобы уменьшить количество уязвимостей, которые позволяют использовать методы LOTL, что включает в себя отключение ненужных протоколов, ограничение доступности сети, ограничение повышенных привилегий, включение по умолчанию защищённого от фишинга MFA, обеспечение защищённости журнала событий, устранение паролей по умолчанию и ограничение динамического выполнения кода.

B. Вторичные моменты

- Направленность на смягчение последствий использования LOTL-методов, когда нецелевым образом применяются легитимные инструменты.
- Поставщики должны нести ответственность за настройки своего программного обеспечения по умолчанию и соблюдение принципа наименьших привилегий.
- Производителям ПО рекомендуется сокращать количество уязвимостей, которыми можно воспользоваться, и брать на себя ответственность за обеспечение безопасности своих клиентов.
- Стратегии сетевой защиты включают мониторинг необычных системных взаимодействий, повышения привилегий и отклонений от обычных административных действий.

- Организациям следует создать и поддерживать инфраструктуру для сбора и систематизации данных для обнаружения методов LOTL, адаптированную к их конкретному ландшафту рисков и ресурсным возможностям

II. Преимущества и недостатки

В анализируемом документе излагается комплексный подход к усилению защиты кибербезопасности от тактики LOTL. Этот подход включает рекомендации по обнаружению, централизованному протоколированию, поведенческому анализу, обнаружению аномалий и упреждающему поиску.

Несмотря на то, что предлагаемые решения обладают значительными преимуществами, организации также должны учитывать потенциальные недостатки и ограничения. Эффективное внедрение требует тщательного планирования, распределения ресурсов и постоянной корректировки с учётом меняющегося ландшафта угроз.

A. Преимущества

- **Расширенные возможности обнаружения**: внедрение комплексной и детализированной системы регистрации событий наряду с централизованным управлением событиями значительно повышает способность организации обнаруживать вредоносные действия. Такой подход позволяет анализировать поведение, обнаруживать аномалии и осуществлять упреждающий поиск, обеспечивая надёжную защиту от методов LOTL.
- **Улучшенная система безопасности**: рекомендуются различные меры, предоставляемые поставщиком или отраслевыми стандартами, сведение к минимуму запущенных служб и защита сетевых коммуникаций с целью сокращения векторов атаки.
- **Повышенная прозрачность**: централизованное управление событиями позволяет выявлять закономерности и аномалии с течением времени. Такой подход в отношении сетевых и системных действий способствует упреждающему обнаружению потенциальных угроз.
- **Эффективное использование ресурсов**: автоматизация анализа журналов и поиска информации повышает эффективность этих процессов, позволяя организациям лучше использовать свои ресурсы. Автоматизированные системы могут сравнивать текущие действия с установленными показателями поведения, с учётом особого внимания привилегированным учётным записям и критически важным активам.
- **Стратегическая сегментация сети**: улучшение сегментации сети и мониторинга ограничивает возможности распространения угрозы, уменьшая "радиус поражения" доступных систем в случае компрометации. Такой стратегический подход помогает сдерживать угрозы и сводит к минимуму потенциальный ущерб.

B. Недостатки/Ограничения

- **Ресурсоёмкость**: реализация рекомендуемых мер по обнаружению и усилению защиты может требовать значительных инвестиций в технологии и обучение персонала. Небольшим организациям будет сложно выделить необходимые ресурсы.
- **Сложность реализации**: создание и поддержание инфраструктуры для детальной регистрации событий и анализа является сложной задачей. Организации могут столкнуться с трудностями при эффективной настройке этих систем и управлении ими, особенно в разнообразных и динамичных ИТ-средах.
- **Снижение эффективности от систем оповещения**: хотя целью предлагаемых решений является снижение избытка оповещений, их огромный объем, генерируемых комплексными системами регистрации и обнаружения аномалий, может привести к переутомлению сотрудников службы безопасности и пропуску важных оповещений.
- **Ложноположительные и отрицательные результаты**: системы анализа поведения и обнаружения аномалий могут формировать ложноположительные и отрицательные результаты, что приводит к ненужным расследованиям инцидентов или пропущенным угрозам. Точная настройка этих систем для сведения к минимуму неточностей требует постоянных усилий и опыта.
- **Зависимость от поддержки поставщиков**: эффективность мер по усилению защиты и безопасных конфигураций часто зависит от поддержки и рекомендаций, предоставляемых поставщиками программного обеспечения. Организации могут столкнуться с ограничениями, если поставщики не уделяют приоритетного внимания безопасности или не предоставляют адекватных рекомендаций по усилению защиты.

III. LIVING OFF THE LAND

Методы LOTL представляют собой стратегию киберугроз, при которой злоумышленники используют нативные инструменты и процессы, уже присутствующие в среде атакуемой цели. Такой подход позволяет органично сочетаться с обычной деятельностью системы, значительно снижая вероятность обнаружения. Эффективность LOTL заключается в её способности использовать инструменты, которые не только уже развёрнуты, но и пользуются доверием в среде, тем самым обходя традиционные меры безопасности, которые могут блокировать или помечать незнакомое или вредоносное программное обеспечение.

Методы LOTL не ограничены каким-либо одним типом среды; они эффективно используются в локальных, облачных, гибридных средах Windows, Linux и macOS.

Такая универсальность отчасти объясняется тем, что злоумышленники предпочитают избегать затрат и усилий, связанных с разработкой и развёртыванием пользовательских инструментов. Вместо этого упор делается на повсеместное применение и доверие к типовым, популярным и нативным инструментам.

A. *Среды Windows*

В корпоративных Windows-средах, методы LOTL особенно распространены из-за широкого использования нативных инструментов, служб и функций операционной системы и доверия к ним.

B. *macOS и гибридные среды*

В этом случае злоумышленники используют нативные скрипт-среды, встроенные инструменты, системные конфигурации и бинарные файлы. Стратегия аналогична стратегии в средах Windows, но адаптирована к уникальным аспектам macOS. В гибридных средах, сочетающих физические и облачные системы, злоумышленники все чаще применяют сложные методы LOTL для использования преимуществ систем обоих типов.

C. *Известные Эксплойты*

Применение эксплоитов хорошо представлено на ресурсах:

- Репозиторий проекта LOLBAS на GitHub предлагает информацию о том, как жить за счёт обычных бинарных файлов, скриптов и библиотек.
- Такие веб-сайты, как gtfobins.github.io, loobins.io и loldrivers.io, предоставляют списки бинарных файлов Unix, macOS и Windows соответственно, которые используются в методах LOTL.

D. *ПО удалённого доступа сторонних производителей*

Помимо нативных инструментов, атакующие также используют ПО удалённого доступа сторонних производителей в следующих категориях: удалённый мониторинг и управление, управление конфигурацией конечных устройств, EDR, управление исправлениями, системы управления мобильными устройствами и инструменты управления базами данных. Эти инструменты, предназначенные для администрирования и защиты доменов, обладают встроенной функциональностью, которая может выполнять команды на всех клиентских узлах в сети, включая такие важные, как контроллеры домена. Также стоит обратить внимание на наборы привилегий, которые требуются этим инструментам для системного администрирования.

IV. Параметры безопасности и избыток уведомлений систем оповещения

Одной из основных выявленных проблем является отсутствие базовых параметров безопасности в организациях, что приводит к выполнению LOLBin без обнаружения аномальной активности. Кроме того, организациям часто не удаётся корректно настроить инструменты обнаружения, что приводит к огромному количеству оповещений, которыми трудно управлять и на которые трудно реагировать. Это усугубляется автоматизированными системами, выполняющими действия с высокими привилегиями, которые могут завалить аналитиков событиями журнала, если их не классифицировать должным образом.

A. *Проблемы с распознаванием вредоносной активности*

Даже организациям со зрелыми передовыми практиками бывает трудно отличить вредоносную активность LOTL от легитимного поведения:

- LOLBins обычно используются ИТ-администраторами и поэтому являются доверительными, что может приводить к заблуждению безопасности для всех пользователей.
- Существует ошибочное представление о том, что легитимные инструменты ИТ-администрирования безопасны априори, что приводит к политикам "разрешения", которые расширяют возможности атаки.
- Исключения для таких инструментов, как PsExec, из-за их регулярного использования администраторами могут быть использованы злоумышленниками для скрытого распространения.

B. *Разрозненные операции и ненастроенные системы EDR*

Информация складывается из опыта redteam и групп реагирования на инциденты в отношении специалистов по сетевой безопасности:

- Обособленная работа от других ИТ-команд препятствует формированию поведенческих пользовательских признаков, устранению уязвимостей и расследования аномального поведения.
- Использование ненастроенных систем обнаружения и EDR и индикаторов компрометации (IOCs), которые могут приводить к отсутствию оповещений о действиях злоумышленников для предотвращения обнаружения.

C. *Конфигурации системы регистрации событий и политики внесения в разрешенные списки*

Недостатки в конфигурациях систем регистрации событий и политиках управления списками разрешений ещё больше усложняют обнаружение действий LOTL:

- Конфигурации систем регистрации событий по умолчанию часто не позволяют фиксировать все соответствующие действия, и журналы из многих приложений требуют дополнительной обработки.
- Политика списков разрешений для диапазонов IP-адресов, принадлежащих хостинг-провайдерам и облачным провайдерам, может непреднамеренно обеспечить «прикрытие для злоумышленников».

D. *Защита устройств macOS*

Несмотря на то, что устройства macOS изначально считаются безопасности, они также требуют настройки:

- В macOS отсутствуют стандартизированные рекомендации по повышению надёжности системы, что приводит к развёртываниям с настройками по умолчанию, которые могут быть небезопасными.
- Презумпция безопасности macOS может привести к отмене приоритетов стандартных мер безопасности и внесение приложений в списки разрешённых.
- В средах со смешанными операционными системами низкая представленность устройств macOS может привести к недостаточному вниманию к их безопасности, что делает их более уязвимыми для вторжений.

V. Возможности для детектирования

A. *Детализированные журналы событий*

- **Внедрение комплексной системы регистрации событий**: решающее значение имеет создание механизмов регистрации всех ИБ-событий на разных платформах и обеспечение агрегирования журналов в централизованном хранилище для предотвращения.
- **Ведение журнала в облачной среде**: для облачных сред важно регистрировать различные события ввиду их бо́льшего количества и настроить политики управления журналами событий для всех облачных служб, особенно редко используемых с целью обнаружения действий злоумышленников.
- **Детализация событий безопасности**: включение детализации событий, таких как командные строки, действия PowerShell и отслеживание событий WMI, обеспечивает более глубокое представление об использовании инструмента в среде, помогая обнаруживать вредоносные действия LOTL.

B. *Установление поведенческих ориентиров*

- **Отслеживание отклонений в параметрах**: отслеживание параметров установленных инструментов, программного обеспечения, поведения учётной записи и сетевого трафика позволяет защитникам выявлять отклонения, которые могут указывать на вредоносную активность.
- **Мониторинг сети и поиск угроз**: улучшение мониторинга сети, расширение хранилища журналов и углубление тактики поиска угроз жизненно важны для выявления длительного присутствия атакующих.

C. *Автоматизация и эффективность*

- **Использование автоматизации**: использование автоматизации для постоянного изучения журналов и сравнения текущих действий с установленными параметрами поведения повышает эффективность поиска, особенно с акцентом на привилегированные учётные записи и критически важные активы.

D. *Снижения «шума» от системы оповещения*

- **Совершенствование инструментов мониторинга**: важно совершенствовать инструменты мониторинга и механизмы оповещения, чтобы проводить различие между типичными административными действиями и поведением, связанным с угрозой, сосредоточив внимание на предупреждениях, которые с наибольшей вероятностью указывают на подозрительные действия.

E. *Использование UEBA*

- **Аналитика поведения пользователей и организаций (UEBA)**: использование UEBA для анализа и сопоставления действий в нескольких источниках данных помогает выявлять потенциальные инциденты безопасности, которые могут быть пропущены традиционными инструментами, и профилировать поведение пользователей для обнаружения внутренних угроз или скомпрометированных учётных записей.

F. *Особенности облачных технологий*

- **Проектирование облачной среды**: проектирование облачной среды для обеспечения надлежащего разделения основных и дополнительных журналов позволяет лучше отслеживать потенциальные действия LOTL.

VI. Hardening-Стратегии

Hardening-стратегии направлены на сокращение количества возможных атак и повышение уровня безопасности критически важной инфраструктуры.

A. *Рекомендации*

Рекомендации по усилению защиты от вендоров и отраслей: организациям следует усиливать конфигурации программного обеспечения и систем на основе рекомендаций по защите от поставщиков или от отрасли, сектора или правительства, например, от NIST, чтобы уменьшить количество векторов атаки.

1) *Для конкретной платформы:*

- **Windows**: применение обновления и исправления для системы безопасности от Microsoft, руководства по базовым показателям безопасности Windows или тестам CIS, ужесточение часто используемых служб, такие как SMB и RDP, и отключение ненужных служб и функций.
- **Linux**: контроль за разрешениями для работы с бинарными файлами и использование стандартов Red Hat Enterprise Linux.
- **macOS**: регулярные обновления и применение исправлений системы, а также встроенных функций безопасности, такие как Gatekeeper,

XProtect и FileVault, и рекомендаций macOS Security Compliance Project.

2) Повышение надежности облачной инфраструктуры:

- **Microsoft Cloud**: применение руководств CISA по настройкам безопасности Microsoft 365 в различных облачных службах Microsoft.
- **Google Cloud**: применение руководств по настройке безопасности Google Workspace Security от CISA для настройки облачных сервисов Google.
- **Универсальные меры защиты**: сведение к минимуму количество запущенных служб, применение принципа наименьших привилегий и защитите сетевые коммуникации.
- **Защита критически важных активов**: применение мер по усилению защиты критически важных активов, таких как ADFS и ADCS, и ограничение приложений и служб, которые могут использоваться или к которым они могут получить доступ.
- **Средства администрирования**: применение предотвращающих повторное использование скомпрометированных учётных данных средств.

B. Список разрешенных приложений

Ограничение выполнения: внедрение списка разрешений приложений как для пользователей, так и администраторов с целью улучшения мониторинга и уменьшения объёма оповещений.

1) Список разрешений для конкретной платформы:

- **macOS**: использование параметров Gatekeeper для предотвращения выполнения неподписанных или неавторизованных приложений.
- **Windows**: использование AppLocker и Windows Defender Application Control для управления исполняемыми файлами, скриптами, MSI-файлами, библиотеками DLL и другими упакованными приложениями.

C. Сегментация сети и мониторинг

- **Ограничение распространения**: реализация сегментации сети для ограничения доступа пользователей минимально необходимыми приложениям и службам, в т.ч. снижения влияния скомпрометированных учётных данных.
- **Анализ сетевого трафика**: применение инструментов для мониторинга трафика между сегментами и размещение сетевые датчики в критических точках для всестороннего анализа трафика.
- **Анализ метаданных сетевого трафика**: применение анализаторов трафика, например Zeek, и интеграция с NID-решениями, например Snort или Suricata.

D. Элементы управления аутентификацией

- **Защита от фишинга**: использование MFA во всех системах, особенно для привилегированных учётных записей.
- **Управление привилегированным доступом (PAM)**: развёртывание надёжных PAM-решений с доступом и элементами управления на основе временного фактора, дополненных ролевым управлением доступа (RBAC).
- **Облачное управление идентификацией и доступом к учётным данным (ICAM)**: применение строгих политик ICAM, аудит конфигураций и смена ключей доступа.
- **Проверка файла Sudoers File Review**: для macOS и Unix регулярная проверка файла sudoers на наличие некорректных настроек в рамках принципа наименьших привилегий.

E. Архитектура нулевого доверия

В качестве долгосрочной стратегии внедряется архитектура с нулевым доверием, чтобы гарантировать, что бинарные файлы и учётные записи не являются доверенными и привилегированными по умолчанию.

F. Дополнительные рекомендации

- **Комплексная проверка при выборе поставщика**: выбор поставщиков с надёжными принципами проектирования и привлечение их к ответственности за конфигурации их программного обеспечения по умолчанию.
- **Аудит ПО удалённого доступа**: аудирование ПО удалённого доступа и применение лучших практик для обеспечения безопасности удалённого доступа.
- **Ограничение исходящего подключения к Интернету**: ограничение доступа к Интернету для внутренних серверов и контроля исходящих подключений для основных служб.

VII. Рекомендации по обнаружению угроз

В рамках рекомендаций предлагаются регулярные проверки инвентаризации системы для выявления поведения злоумышленников, которое может быть пропущено журналами событий из-за некорректных конфигураций. Организациям рекомендуется включить регистрацию всех событий, связанных с безопасностью, включая действия командной строки, системные вызовы и журналы аудита на всех платформах, чтобы улучшить обнаружение вредоносной активности LOTL.

A. Сетевые журналы

Обнаружение LOTL-методов с помощью сетевых журналов представляет собой проблемы из-за преходящего характера сетевых артефактов и сложности распознавания вредоносной активности от легитимного поведения. В отличие от артефактов хоста, которые часто можно обнаружить, если только атакующий намеренно не удалит их, сетевые артефакты являются производными от сетевого

трафика, временными и требуют надлежащей настройки систем управления событиями для их отслеживания. Без соответствующих датчиков для регистрации сетевого трафика невозможно наблюдать за активностью LOTL.

B. *Показатели активности LOTL*

Обнаружение активности LOTL включает в себя поиск набора возможных индикаторов для формирования связанных поведенческих сетевых признаков в трафике.

- **Просмотр журналов брандмауэра**: Заблокированные попытки доступа в журналах брандмауэра могут сигнализировать о компрометации, особенно в должным образом сегментированной сети. Попытки обнаружения сети и сопоставления внутри неё также могут указывать на активность LOTL. Важно различать обычное поведение инструмента управления сетью и аномальное.

- **Исследование аномальных признаков в трафике**: изучение определённых типов трафика, такие как запросы LDAP от хостов Linux, не присоединённых к домену, запросы SMB из разных сегментов сети или запросы доступа к базе данных с рабочих станций пользователей, которые должны выполняться только внешними серверами, с конечной целью отличить легитимное приложения от вредоносных запросов.

- **Изучение журналов сетевых служб на хост-машинах**: журналы таких служб, как Sysmon и IIS, на хост-машинах могут предоставить информацию о взаимодействиях веб-сервера, транзакциях FTP и других сетевых действиях. Эти журналы содержат ценный контекст и детали, которые могут быть недоступны традиционным сетевым устройствам.

- **Объединение журналов сетевого трафика с журналами на базе хоста**: этот подход позволяет включать дополнительную информацию, такую как учётная запись пользователя и сведения о процессе. Расхождения между артефактами назначения и внутри сети могут указывать на вредоносный трафик.

C. *Журналы событий приложений, безопасности и системных событий*

Системы регистрации событий по умолчанию часто не позволяют фиксировать все необходимые события, потенциально оставляя пробелы в видимости вредоносных действий. Определение приоритета журналов и источников данных, которые с большей вероятностью выявят вредоносную активность LOTL, имеет решающее значение для эффективного обнаружения и реагирования.

D. *Журналы аутентификации*

Журналы аутентификации играют важную роль в выявлении попыток несанкционированного доступа и отслеживании действий пользователей по сети. Регистрация всех операций, включая вызовы API и входы конечных пользователей, с помощью таких сервисов, как Amazon Web Services CloudTrail, Azure Activity Log и Google Cloud Audit Logs. Эти журналы могут предоставить ценную информацию о потенциальных действиях LOTL, выявляя необычные схемы доступа или попытки использования механизмов аутентификации.

Надёжная стратегия разграничения привилегий необходима для идентификации методов LOTL по журналам аутентификации. Такие практики, как ограничение доступа учётных записей администраторов домена только к контроллерам домена и использование рабочих станций привилегированного доступа (PAWs) и наличие MFA могут свести к минимуму доступ к учётным данным и усилить сегментацию сети.

E. *Регистрация событий на хосте*

Sysmon и другие инструменты регистрации хостовых событий обеспечивают детальную визуализацию системных действий о создании процессов, сетевых подключениях и изменениях файловой системы, эти инструменты с целью обнаружения и расследования подозрительных активностей и поведенческих признаков.

1) *Установление исходных условий и обеспечение защиты журнала*

Основополагающим шагом в обнаружении аномального или потенциально вредоносного поведения является установление условий запуска инструментов и событий. Это включает в себя понимание механизмов безопасности операционных систем для выявления отклонений, которые могут указывать на угрозу безопасности. Также важно полагаться на защищённые журналы, которые менее подвержены подделке злоумышленниками. Например, в то время как файлы Linux .bash_history могут быть изменены непривилегированными пользователями, журналы аудита системного уровня более безопасны и обеспечивают надёжную запись действий.

2) *Использование Sysmon в средах Windows*

Sysmon, инструмент мониторинга системы Windows, предоставляет детальную информацию о таких действиях, как создание процессов, сетевые подключения и модификации реестра. Подробное протоколирование имеет неоценимое значение для служб безопасности при поиске и выявлении случаев неправильного использования легитимных инструментов. Ключевые стратегии включают:

- Использование свойства OriginalFileName для идентификации переименованных файлов, которые могут указывать на вредоносную активность (для большинства утилит Microsoft исходные имена файлов хранятся в заголовке PE).

- Внедрение методов обнаружения для выявления использования утилит командной строки и скриптов, особенно использующих альтернативные потоки данных (ADS) - мониторинг определённых аргументов командной строки или синтаксиса, используемых для взаимодействия с ADS.

3) *Стратегии обнаружения*

Усовершенствование конфигураций Sysmon для анализа с упором на шаблоны, указывающие на обфускацию, может

помочь выявить попытки обойти средства мониторинга безопасности, например использование управляющих символов, объединение команд и использование кодировки Base64.

4) Мониторинг подозрительных цепочек процессов

Мониторинг подозрительных цепочек процессов, например связанных с Microsoft Office и процессами создания скриптов, является ключевым показателем активности LOTL, т.к. приложения Office редко запускают процессы (cmd.exe, PowerShell, wscript.exe или cscript.exe).

5) Интеграция журналов с SIEM-системами

Интеграция журналов Sysmon с SIEM-системами с целью применения правил корреляции может значительно улучшить обнаружение атак путём автоматизации процесса обнаружения и применения аналитики для выявления сложных поведенческих моделей вредоносной активности.

6) Рекомендации по работе с Linux и macOS

На компьютерах с Linux использование Auditd или Sysmon и интеграция этих журналов с платформой SIEM могут значительно улучшить обнаружение аномальных действий. Для macOS использование таких инструментов, как Santa, система авторизации с открытым исходным кодом, может помочь отслеживать выполнение процессов и обнаруживать аномальное поведение производительных приложений

F. Просмотр Конфигураций

Регулярный анализ и обновление системных конфигураций необходимы для обеспечения того, чтобы меры безопасности оставались эффективными против возникающих угроз. Это включает проверку того, что параметры систем регистрации событий надлежащим образом настроены для сбора соответствующих данных и что средства контроля безопасности соответствуют современным передовым практикам. Организациям также следует оценить использование списков разрешений и других механизмов контроля доступа для предотвращения злоупотребление легитимными инструментами злоумышленниками.

Регулярные проверки конфигураций хостов на соответствие установленным базовым показателям необходимы для выявления признаков компрометации, и включают изменения в установленном программном обеспечении, конфигурации брандмауэра и обновления основных файлов, таких как файл Hosts, который используется для разрешения DNS. Проверки могут выявить несоответствия, которые сигнализируют о несанкционированных модификациях или присутствии вредоносного программного обеспечения.

- **Обход стандартных журналов событий**: известно, что атакующие обходят стандартные журналы событий, напрямую внося изменения в реестр для регистрации служб и запланированных задач. Такой подход не регистрируется в стандартных системных событиях, что делает его способом сокрытия активностей.
- **Системные инвентаризационные аудиты**: проведение регулярных системных инвентаризационных аудитов является упреждающей мерой для выявления поведения злоумышленников, которое могло быть пропущено журналами событий по различным причинам, а также гарантирует, что любые изменения в системе санкционированы и учтены.

G. Поведенческий анализ

Сравнение активности с обычным поведением пользователя позволяет говорить об обнаружении аномалий. Необычное поведение, на которое следует обратить внимание, например включает нетиповое время входа в систему, доступ вне ожидаемого рабочего графика или праздничных перерывов, быструю последовательность или большое количество попыток доступа, необычные пути доступа, одновременные входы в систему из нескольких мест.

H. NTDSUtil.exe и PSExec.exe

Особое внимание уделяется выявлению неправомерного использования NTDSUtil.exe и PSExec.exe инструментов, которые, хотя и являются легитимными, часто используются злоумышленниками в злонамеренных целях, например попытки сбросить учётные данные или распространяться по сети в направлении. Сосредоточив внимание на поведенческом контексте использования этих инструментов, организации могут более эффективно проводить различие между легитимными и вредоносными действиями.

1) Процесс эксплуатации

Обычная тактика заключается в создании теневой копии системного диска на томе, обычно с помощью vssadmin.exe с помощью таких команд, как Create Shadow /for=C:. Это действие создает моментальный снимок текущего состояния системы, включая базу данных Active Directory. После этого ntdsutil.exe используется для взаимодействия с этой копией с помощью определённой последовательности команд (ntdsutil snapshot “activate instance ntds” create quit quit). Затем злоумышленники получают доступ к теневой копии, чтобы извлечь файл ntds.dit из указанного каталога. Эта последовательность предназначена для извлечения конфиденциальных учётных данных, таких как хэшированные пароли, из Active Directory, что позволяет полностью скомпрометировать домен.

2) Обнаружение и реагирование

Для обнаружения такого использования и реагирования на него крайне важно понимать контекст ntdsutil.exe действий и проводить различие между легитимным административным использованием и потенциальным злонамеренным использованием. Основные источники журналов и стратегии мониторинга включают:

- **Журналы командной строки и создания процессов**: журналы безопасности (**идентификатор события 4688**) и журналы Sysmon (**идентификатор события 1**) предоставляют информацию о выполнении ntdsutil.exe команд. Необычное или нечастое использование ntdsutil.exe

для создания моментальных снимков может указывать на подозрительную активность.

- **Журналы создания файлов и доступа к ним**: мониторинг событий создания файлов (**идентификатор события Sysmon'a 11**) и попыток доступа к конфиденциальным файлам, таким как NTDS.dit (**идентификатор события 4663**), могут предоставить дополнительный контекст для процесса создания моментальных снимков и доступа.

- **Журналы использования привилегий**: идентификатор события 4673 в журналах, указывающий на использование привилегированных служб, может говорить о потенциальном злоупотреблении, когда оно связано с выполнением ntdsutil.exe команд.

- **Журналы сетевой активности и аутентификации**: журналы могут содержать информацию о одновременных удалённых подключениях или передачах данных, потенциально указывая на попытки эксфильтрации данных. Журналы аутентификации также важны для идентификации исполнителя команды ntdsutil.exe и оценки того, соответствует ли использование типичному поведению администратора.

3) Комплексный анализ PSExec.exe

PSExec.exe, компонент пакета Microsoft PsTools, представляет собой мощную утилиту для системных администраторов, предлагающую возможность удалённого выполнения команд в сетевых системах, часто с повышенными привилегиями. Однако его универсальность также делает его излюбленным инструментом у APT-групп.

4) Роль PSExec.exe в киберугрозах

PSExec.exe обычно используется для удалённого администрирования и выполнения процессов в разных системах. Его способность работать с системными привилегиями делает его особенно привлекательным для вредоносного использования, например для выполнения одноразовых команд, направленных на изменение системных конфигураций, таких как удаление конфигураций прокси-порта на удалённом хосте с помощью команд типа:

"C:\pstools\psexec.exe" {REDACTED} -s cmd /c "cmd.exe /c netsh interface portproxy delete v4tov4 listenaddress=0.0.0.0 listenport=9999"

5) Стратегии обнаружения

Для эффективного противодействия злонамеренному использованию PSExec.exe сетевые защитники должны использовать различные журналы, которые дают представление о выполнении команд и более широком контексте операции:

- **Журналы командной строки и создания процессов**: Журналы безопасности (**идентификатор события 4688**) и журналы Sysmon (**идентификатор события 1**) полезны для отслеживания выполнения PSExec.exe и связанных с ними команд. В этих журналах подробно описывается использованная командная строка, определяющая природу и «намерения» процесса.

- **Журналы использования привилегий и явных учётных данных**: журналы безопасности **Идентификатор события 4672**) документируют случаи, когда новым входам в систему назначаются особые привилегии, что крайне важно, когда PsExec выполняется с переключателем -s для системных привилегий. Идентификатор события 4648 фиксирует явное использование учётных данных, указывая, когда PsExec запускается с определёнными учётными данными пользователя.

- **Sysmon регистрирует сетевые подключения и изменения реестра**: идентификатор события 3 Sysmon регистрирует сетевые подключения, что является центральным элементом функции удалённого выполнения PsExec. Идентификаторы событий 12, 13 и 14 отслеживают изменения реестра, включая удаления (Идентификатор события 14) разделов реестра, связанных с выполненной командой Netsh, предоставляя доказательства изменений конфигурации системы.

- **Журналы аудита реестра Windows**: в журналы записываются изменения разделов реестра, содержащие информацию, такую как временная метка изменений, учётная запись, под которой были внесены изменения (часто системная учётная запись из-за переключателя PsExec -s), и конкретные изменённые или удалённые значения реестра.

- **Журналы сети и брандмауэра**: анализ сетевого трафика, особенно трафика SMB, характерного для использования PsExec, и журналов брандмауэра в целевой системе может выявить подключения к общим ресурсам администрирования и изменения конфигурации сети системы. Журналы коррелируют со временем выполнения команды, предоставляя дополнительный контекст для действия.

VIII. Стратегии для скомпрометированных сетей

В случае обнаружения факта компрометации необходимо применение защитных контрмер.

A. Действия немедленного реагирования

- Сброс учётных данных для привилегированных и непривилегированных учётных записей в пределах границ доверия каждой скомпрометированной учётной записи.

- Принудительный сброс пароля, отзыв и выдача новых сертификатов для всех учётных записей и устройств.

B. Действия, относящиеся к среде Windows:

- При подозрении на доступ к Контроллеру домена (DC) или Active Directory (AD) сброс паролей всех локальных учётных записей, включая Guest,

HelpAssistant, DefaultAccount, System, Administrator и krbtgt. Учётную запись krbtgt, которая обрабатывает запросы на регистрацию Kerberos, следует дважды сбросить для обеспечения безопасности из-за истории с двумя паролями.

- Если есть подозрение, что файл ntds.dit подвергался эксфильтрации, требуется сброс пароля всех пользователей домена.
- Просмотр и коррекция политики доступа для временного отзыва или уменьшения права доступа для затронутых учётных записей и устройств.
- Сброс учётных данных учётной записи без повышенных прав доступа: если доступ атакующего ограничен правами, сброс соответствующих учётным данным ключа доступа и отслеживание дальнейших признаков несанкционированного доступа, особенно к учётным записям администраторов.

C. *Аудит конфигурации сети и устройств*

- **Аудит сетевых устройств и пограничных устройств**: проверка наличия признаков несанкционированных или вредоносных изменений конфигурации. Если изменения обнаружены:
  - Требуется изменения всех учётных данных, используемых для управления сетевыми устройствами, включая ключи и строки, обеспечивающие функции сетевого устройства.
  - Обновление всех прошивок и программного обеспечения до последних версий.

D. *Использование инструмента удалённого доступа*

Минимизация удалённого доступа и контроль: следование рекомендациям по обеспечению безопасности средств и протоколов удалённого доступа, включая рекомендации по безопасности программного обеспечения удалённого доступа и безопасному использованию PowerShell.

IX. Рекомендации для производителей ПО

A. *Минимизация векторов атаки*

Производителям ПО настоятельно рекомендуется минимизировать возможности атаки путём выполнения различных действий: отключение ненужных протоколов по умолчанию, ограничение количества процессов и программ, запущенных с повышенными привилегиями, и принятие упреждающих мер по ограничению возможностей участников использовать нативные функциональные возможности для вторжений.

B. *Внедрение системы безопасности в SDLC*

Безопасность должна быть встроена в архитектуру продукта на протяжении всего жизненного цикла разработки программного обеспечения (SDLC). Такая упреждающая интеграция гарантирует, что соображения безопасности станут не второстепенной задачей, а фундаментальным компонентом продукта от начала разработки до развертывания.

C. *Обязательная многофакторная аутентификация (MFA)*

Производителям следует установить MFA, в идеале защищенный от фишинга, для привилегированных пользователей и сделать его функцией по умолчанию, а не необязательной. Этот шаг значительно повышает безопасность учётных записей пользователей, особенно тех, которые имеют повышенный доступ.

D. *Уменьшение hardening-действий*

Объём действий, прилагаемых к объектам защиты, следует отслеживать и уменьшать. По мере выпуска новых версий программного обеспечения целью должно быть уменьшение размера этих руководств с течением времени путем интеграции их компонентов в качестве конфигурации продукта по умолчанию.

E. *Учёт пользовательского опыта*

Необходимо учитывать влияние настроек безопасности на работу пользователя. В идеале наиболее безопасная настройка должна быть интегрирована в продукт по умолчанию, а при необходимости настройки опция должна быть защищена от распространённых угроз. Такой подход снижает когнитивную нагрузку на конечных пользователей и обеспечивает широкую защиту.

F. *Удаление паролей по умолчанию*

Пароли по умолчанию следует полностью исключить, или сформировать, или установить при первой установке, а затем периодически менять. Такая практика предотвращает использование паролей по умолчанию в качестве удобной точки входа для злоумышленников.

G. *Ограничение динамического выполнения кода*

Динамическое выполнение кода, хотя и обеспечивает универсальность, представляет собой уязвимое место для атаки. Производителям следует ограничить или удалить возможность динамического выполнения кода из-за высокого риска и сложности обнаружения связанных с ним индикаторов компрометации (IoC).

H. *Удаление фиксированных учётных данных*

Приложения и скрипты, содержащие информацию об учётных данных в виде открытого текста (hardcode), представляют значительный риск для безопасности. Удаление таких учётных данных важно для предотвращения использования их злоумышленниками для доступа к ресурсам и расширения своего присутствия в сети.