

В перспективе до 2035 года успех этой стратегии будет зависеть от того, насколько глубоко принципы экологической ответственности проникнут во все уровни принятия решений – от государственных программ до частных инвестиций.

СПИСОК ИСТОЧНИКОВ

1 О Стратегии обращения с отработавшим ядерным топливом Белорусской атомной электростанции : постановление Совета Министров Респ. Беларусь от 22 авг. 2019 г. № 558. – URL: <https://etalonline.by/document/?regnum=c21900558> (дата обращения: 03.05.2026).

2 О Национальной стратегии развития экономики замкнутого цикла до 2035 года : постановление Совета Министров Респ. Беларусь от 29 мая 2024 г. № 393. – URL: <https://pravo.by/document/?guid=3871&p0=C22400393> (дата обращения: 03.05.2026).

3 ОАО «Гродно Азот»: планы по модернизации до 2026 года. – URL: <https://www.sb.by/articles/uznali-za-schet-chego-grodno-azot-planiruet-narastit-obemy-proizvodstva-v-2026-godu.html?amp=1> (дата обращения: 03.05.2026).

4 Стратегия в области охраны окружающей среды Республики Беларусь на период до 2035 года. – URL: https://krichev.gov.by/downloads/actual/strategy_2035.pdf (дата обращения: 03.05.2026).

Получено 27.05.2026

ISSN 2227-1155. Сборник студенческих научных работ.
Вып. 31. Гомель, 2026

УДК 004.056+004.451

Н. А. АМЕЛЬЧЕНКО, М. А. ЖЕСТКИН, В. А. ГУБСКИЙ (ЭМ-31)

Научный руководитель – ст. преп. *В. Е. МИНИН*

МЕТОДЫ ОБХОДА СРЕДСТВ БЕЗОПАСНОСТИ И ЗАЩИТЫ С ИСПОЛЬЗОВАНИЕМ ШТАТНЫХ СРЕДСТВ ОПЕРАЦИОННЫХ СИСТЕМ

Рассматривается концепция Living Off The Land (LOTL), предполагающее использование легитимных системных инструментов для проведения кибератак. Такие техники затрудняют обнаружение злоумышленников, так как применяют встроенные средства операционной системы, например, PowerShell или Bash. Обсуждаются проекты LOLBAS и GTFOBins, содержащие список таких утилит, и их роль в обходе защиты, повышении привилегий и скрытии следов. Анализируются преимущества, сложности и методы защиты от LOTL-атак, подчеркивается их универсальность и необходимость комплексных мер безопасности.

Словосочетание Living Off The Land (LOTL, буквально «кормиться с земли» или, что точнее по смыслу, «работать подручными средствами») достаточно точно отражает суть одноименного подхода к проведению кибератак. Такие атаки также называют LOTL-атаками или LOLBAS-атаками. Их клю-

чая особенность заключается в использовании штатных средств операционной системы для выполнения вредоносных действий [1–3].

В отличие от традиционных атак злоумышленнику не обязательно разрабатывать собственное вредоносное программное обеспечение для загрузки или запуска вредоносного кода. Современные операционные системы уже содержат множество инструментов, способных выполнять необходимые действия: запускать программы, скачивать файлы, изменять настройки системы и автоматизировать различные процессы. Задача атакующего сводится к тому, чтобы заставить эти инструменты работать в своих интересах.

Одним из наиболее известных инструментов, часто используемых в рамках LOTL-подхода, является PowerShell. Эта оболочка командной строки по умолчанию присутствует в большинстве современных версий Windows и обладает широкими возможностями автоматизации. С ее помощью злоумышленники могут выполнять команды, загружать полезную нагрузку, автоматизировать действия внутри системы и реализовывать другие этапы атаки. Поскольку PowerShell является легитимным системным компонентом, его использование зачастую сложнее обнаружить традиционными средствами защиты. Дополнительным преимуществом для злоумышленников является присутствие данного инструмента в операционных системах Windows по умолчанию.

Для систематизации подобных техник был создан проект LOLBAS (Living Off The Land Binaries and Scripts). Он представляет собой открытый каталог исполняемых файлов и скриптов Windows, которые могут использоваться для обхода механизмов защиты.

По сути проект является справочником легитимных утилит и способов их нестандартного применения. На сайте проекта представлены как сами инструменты, так и примеры их использования для обхода различных ограничений безопасности [3].

Для Unix-подобных операционных систем существует аналогичный проект – GTFOBins [2]. Он представляет собой базу данных стандартных утилит, которые могут применяться для повышения привилегий, обхода ограничений безопасности или выполнения иных действий, не предусмотренных их основным назначением. Как в Windows, так и в Unix-подобных системах многие штатные инструменты обладают гораздо более широкими возможностями, чем принято считать. Именно эти возможности нередко используются злоумышленниками для получения доступа к системе. Поскольку действия выполняются легитимными средствами самой операционной системы, их обнаружение существенно усложняется.

Главным преимуществом LOTL-подхода является использование доверенных программ. Кроме того, злоумышленникам не требуется тратить ресурсы на разработку собственного инструментария. Вредоносная активность маскируется под обычную работу системы, поскольку задействуются те же утилиты, которые регулярно используются операционной системой и администраторами.

Традиционные антивирусные решения нередко оказываются малоэффективными в подобных сценариях, так как запускаемые процессы имеют цифровую подпись и считаются доверенными. С точки зрения системы происходящее может выглядеть как обычные действия пользователя.

Важно отметить, что в большинстве случаев злоумышленники не модифицируют код используемых программ. Поэтому LOTL нельзя рассматривать как эксплуатацию классической программной уязвимости. Речь идет не об ошибке в коде, а о злоупотреблении штатной функциональностью системы.

Характерным примером является утилита CertUtil.exe, предназначенная для работы со службами сертификатов. Одной из ее штатных функций является загрузка сертификатов из сети. Однако злоумышленник может использовать этот механизм для скачивания произвольного файла, например, вредоносного скрипта. После загрузки утилита определит, что полученный файл не является сертификатом, и завершит операцию с ошибкой, однако сам файл уже окажется на компьютере жертвы. Помимо загрузки данных, различные LOLBAS-инструменты могут применяться для повышения привилегий, организации удаленного доступа, закрепления в системе и сокрытия следов деятельности. Среди часто используемых утилит можно выделить cmd.exe, wmic.exe, mshta.exe и rundll32.exe.

В Linux и других Unix-подобных системах также существует множество инструментов, пригодных для реализации аналогичных сценариев. Наиболее известным примером является Bash – командная оболочка и язык сценариев, функционально во многом сопоставимый с PowerShell. Благодаря поддержке автоматизации Bash позволяет выполнять широкий спектр действий внутри системы. Кроме того, в контексте атак часто упоминаются утилиты awk, sed, find, tar, curl и wget.

Несмотря на кажущуюся опасность подобных техник, на практике для получения доступа к критически важным системным ресурсам злоумышленнику зачастую всё равно требуются повышенные привилегии. Поэтому многие LOTL-атаки фактически сводятся к эксплуатации ошибок конфигурации или неосторожных действий пользователей и администраторов, предоставивших избыточные права отдельным программам.

Существуют и исключения. Некоторые системные компоненты могут обладать повышенными привилегиями по умолчанию. Например, в ряде версий Windows фигурировали eventvwr.exe и eudcedit.exe, которые при определенных условиях могли использоваться для выполнения команд с административными правами. Однако подобные примеры уже находятся на границе между классическими LOTL-техниками и эксплуатацией конкретных уязвимостей.

Пример использования eventvwr для UAC Bypass:

```
powershell -c "New-Item -Path 'HKCU:\Software\Classes\mscfile\shell\open\command' -Force; Set-ItemProperty -Path 'HKCU:\Software\Classes\mscfile\shell\open\command' -Name '(default)' -Value 'cmd.exe'"
```

Теперь при запуске eventvwr.exe будет запускаться cmd.exe с правами администратора. Как правило, в реальных атаках LOTL используется совместно с другими методами компрометации. Сначала злоумышленник получает первоначальный доступ к системе или повышает свои привилегии с помощью уязвимости, а затем применяет штатные инструменты операционной системы для дальнейшего развития атаки.

Тем не менее существуют сценарии, в которых административные права не требуются. Например, если целью являются пользовательские данные, доступ к которым разрешен текущему пользователю. Кроме того, использование встроенных инструментов позволяет отказаться от загрузки дополнительного вредоносного программного обеспечения, что делает LOTL-техники особенно востребованными в рамках fileless-атак, где большинство действий выполняется непосредственно в оперативной памяти.

Защита от подобных угроз требует комплексного подхода. В корпоративной среде ключевую роль играют принцип наименьших привилегий и подход allowlisting, предполагающий разрешение запуска только заранее определенного набора программ [4].

Утилиты из списка LOLBAS, не используемые в рабочих процессах организации, рекомендуется полностью блокировать. Даже доверенные системные инструменты должны запускаться с повышенными привилегиями только при наличии обоснованной необходимости.

Для обычных пользователей актуальны те же базовые принципы безопасности: своевременное обновление системы, ограничение прав доступа и контроль запускаемых программ.

Кроме того, важным фактором является снижение собственной привлекательности как цели для злоумышленников. Несмотря на возможность массового применения отдельных LOTL-техник, эффективное использование такого подхода часто требует детального изучения конкретной системы и поиска индивидуальных точек входа, что делает его особенно востребованным в рамках целевых атак.

Не менее важным направлением является расследование уже произошедших инцидентов. Поскольку LOTL-атаки ориентированы на максимальную скрытность, организациям рекомендуется использовать централизованные системы журналирования событий, защищенные от удаления и несанкционированного изменения.

Для повышения эффективности анализа следует минимизировать количество ненужных фоновых процессов и сервисов, уменьшая объем нормальной активности системы. Современные решения по мониторингу безопасности, включая системы анализа поведения пользователей и технологии искусственного интеллекта, способны выявлять отклонения от типичных сценариев работы и своевременно сигнализировать о возможной атаке.

Можно сделать следующие выводы: использование LOTL не является отдельным видом вредоносного программного обеспечения, а демонстриру-

ет универсальный подход к проведению атак с использованием легитимных инструментов операционной системы.

Такие техники отличаются высокой гибкостью и скрытностью, однако требуют глубокого понимания особенностей целевой системы и нередко используются в сочетании с другими методами компрометации. Важно понимать, что LOTL может применяться практически на любом этапе атаки – от получения первоначального доступа до закрепления в системе и сокрытия следов. Поэтому на практике термин «LOTL-атака» используется не всегда. Достаточно того, что злоумышленник на одном из этапов задействует штатный инструмент, например, PowerShell для внесения изменений в реестр и организации автозапуска вредоносного компонента, чтобы данный эпизод рассматривался как применение техники Living off the Land.

СПИСОК ЛИТЕРАТУРЫ

1 Living Off The Land Binaries, Scripts and Libraries. – URL: <https://lolbas-project.github.io/> (date of access: 04.04.2026).

2 Хит-парад LolBins. – URL: <https://www.kaspersky.ru/blog/most-used-lolbins/31557/> (дата обращения: 04.04.2026).

3 LOLBaS. – URL: <https://www.securitylab.ru/glossary/lolbas/> (date of access: 04.04.2026).

4 Как подготовиться к атакам, ведущимся подручными средствами (LOTL). – URL: <https://www.kaspersky.ru/blog/lotl-attacks-detection-hardening-guidance/37163/> (дата обращения: 04.04.2026).

Получено 11.06.2026

ISSN 2227-1155. Сборник студенческих научных работ.

Вып. 31. Гомель, 2026

УДК 658.7/.8

К. Н. АНАЦКО (УЛ-21)

Научный руководитель – ст. преп. *Е. В. МАЛИНОВСКИЙ*

ОПРЕДЕЛЕНИЕ УРОВНЯ ЛОГИСТИЧЕСКОГО СЕРВИСА (УРОВНЯ УДОВЛЕТВОРЕНИЯ СПРОСА ЗАПАСАМИ)

Рассмотрены виды услуг логистического сервиса, предложен подход к оценке уровня логистического сервиса через отношение фактически выполненных услуг к теоретически возможным, обоснован критерий оптимизации по максимуму прибыли с учетом роста затрат при повышении уровня обслуживания.

Важнейшей функцией запасов является обеспечение бесперебойности процесса производства и потребления с учетом колебаний спроса. Уровень