# МЕТОДИКА ОБНАРУЖЕНИЯ LOTL-АТАК ПРИ ПОМОЩИ SIEM-СИСТЕМЫ WAZUH

*Шумченя М.А., Лукашик Л.А., студенты гр. 361402*

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

*Мокеров В.С. – ассистент каф. ЗИ*

**Аннотация.** Статья посвящена исследованию методов обнаружения атак класса Living off the Land (LotL) с использованием SIEM-системы Wazuh. Рассмотрена техника эксплуатации легитимной утилиты mshta.exe в контексте тактики Defense Evasion согласно классификации MITRE ATT&CK. Экспериментально установлено, что штатные механизмы Wazuh не обеспечивают обнаружение данной угрозы без разработки специализированных правил корреляции. Предложена методика составления XML-правил, подтверждённая практической апробацией. Полученные результаты свидетельствуют о необходимости регулярного расширения базы правил корреляции как обязательного условия обеспечения киберустойчивости информационных систем.

**Ключевые слова.** Living off the Land, LolBins, mshta.exe, SIEM, Wazuh, правила корреляции, MITRE ATT&CK.

В современных условиях значительную проблему для систем обнаружения вторжений представляет использование легитимных системных утилит в вредоносных целях, известных как LolBins. (Living Off the Land Binaries and Scripts). LolBins – это термин, используемый в кибербезопасности для обозначения легитимных исполняемых файлов, скриптов или утилит, уже доступных на компьютере пользователя, с помощью которых хакеры выполняют различные вредоносные действия. Вместо того чтобы загружать вредоносные файлы с внешних источников, злоумышленники используют инструменты, которые уже находятся в системе. Таким образом они избегают обнаружения антивирусными программами или другими системами обеспечения безопасности [1].

Данный метод имеет много преимуществ с точки зрения злоумышленника:

– злонамеренная деятельность сочетается с повседневной сетевой и административной деятельностью;

– инструменты, уже установленные на компьютерах, с меньшей вероятностью запускают защиту конечных точек;

– нет необходимости тратить время и ресурсы на разработку собственных вредоносных инструментов;

– такая активность не дает очевидных показателей компрометации, что затрудняет отслеживание вредоносной активности и сравнение атак между организациями;

– многие компании не могут собрать и хранить информацию о мониторинге сети и повседневной сетевой активности достаточно подробно, поэтому невозможно отслеживать эволюцию атаки в реальном времени. Это делает предотвращение атак и смягчение их последствий чрезвычайно сложным [2].

Инструменты Windows, полезные для злоумышленников, обычно называются LolBins или LOLBAS (LOLbinaries and scripts). Наиболее популярными являются PowerShell и rundll32 [3].

Данные инструменты изначально входят в состав операционной системы и предназначены для выполнения административных задач, что позволяет злоумышленникам использовать их для обхода механизмов сигнатурного обнаружения и снижения вероятности выявления подозрительной активности.

В рамках данной работы был проведен эксперимент, направленный на анализ эффективности обнаружения подобных техник средствами системы мониторинга безопасности Wazuh [4].

Wazuh является наиболее широко распространенной платформой кибербезопасности с открытым исходным кодом, объединяющей XDR (Extended Detection and Response) и SIEM (Security Information and Event Management) в одном решении. Он анализирует данные безопасности по конечным точкам, облакам и сетям для обнаружения угроз, реагирования на инциденты и обеспечения соответствия, помогая организациям укреплять свою безопасность посредством непрерывного мониторинга и автоматизации.

Wazuh отслеживает параметры системы и конфигурации приложений, чтобы убедиться, что они соответствуют политикам безопасности, стандартам и/или руководствам по усовершенствованию систем безопасности. Агенты Wazuh проводят периодическое сканирование для выявления неправильных конфигураций или пробелов в безопасности в конечных точках, которые могут быть использованы субъектами угроз. Кроме того, есть возможность настроить эти проверки конфигурации, тем самым адаптируя их, чтобы должным образом соответствовать потребностям организации. Оповещения о безопасности включают рекомендации по лучшей конфигураций с соблюдением нормативных требований [5].

В качестве исследуемой утилиты была выбрана mshta, применяемая для реализации сценария загрузки и последующего исполнения вредоносного файла [6]. mshta - Microsoft HTML (HyperText Markup Language) Application Host. Программа используется для запуска .hta (HTML Application) файлов. Выполнение этого процесса не критично для операционной системы. Однако, если удалить этот файл, это может оказать влияние на стабильную работу Windows. Если запущенное HTML приложение зависло или работает нестабильно, его можно безопасно уничтожить, используя диспетчер задач.

mshta также предоставляет злоумышленникам гибкость для встраивания полезной нагрузки скрипта в любой законный формат файла. Например, характерно встраивать контент HTA в законные двоичные файлы Microsoft (пример - DIALER.EXE). Злоумышленники просто добавляют вредоносный контент HTA в конец файла и mshta.exe сканирует файл до тех пор, пока он не найдет действительное содержимое скрипта HTA. Злоумышленники знают, что полезная нагрузка с меньшей вероятностью будет первоначально обнаружена, если она встроена в законный файл [7].

В MITRE ATT&CK mshta фигурирует в тактике Defense Evasion, Sub-technique of: T1218 [8].

В целях нашей работы, мы сначала эксплуатировали mshta, не написав правила корреляции.

Правила корреляции для Wazuh имеют синтаксис XML (eXtensible Markup Language). При написании правил руководствовались документацией на официальном сайте Wazuh [9] [10].

«mshta.exe http://192.168.100.110:8000/test.hta» – команда, при помощи которой мы имитировали атаку.

Далее после прописания данной команды, смотрели логи Sysmon [11]. На рисунке 1 приведено изображение события.

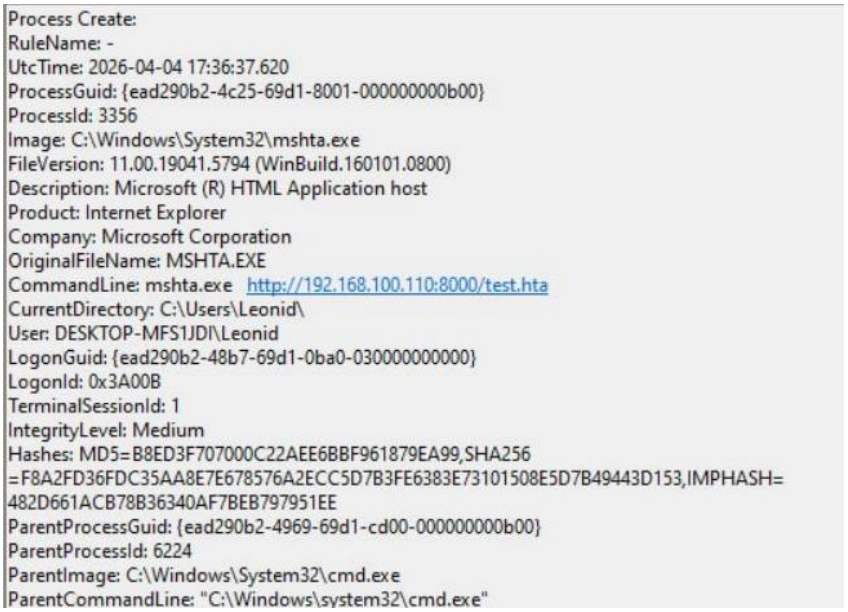


Рисунок 1 – Лог Sysmon

В это же время таких же событий на SIEM нет. На рисунке 2 мы можем видеть, что диапазон времени целые сутки, однако, сработки по mshta мы не видим.


Рисунок 2 – События на SIEM

Далее настроили правила и после повторной имитации атаки, зайдя на SIEM, увидели событие 14 уровня, которое свидетельствует о том, что правило работает. На рисунке 3 представлено правило, на рисунке 4 представлено событие на Wazuh.

```
<group name="lolbins,windows,sysmon,">

  <!-- EID 1: Process Create -->
  <rule id="230001" level="12">
    <if_group>sysmon_event1</if_group>
    <field name="win.eventdata.image" type="pcre2">(?i)\\certutil\.exe$</field>
    <field name="win.eventdata.commandLine" type="pcre2">(?i)(urlcache|decode|encode|-ping|-verify)</field>
    <description>LOLBin: certutil - $(win.eventdata.commandLine)</description>
    <mitre><id>T1105</id><id>T1140</id></mitre>
  </rule>

  <rule id="230002" level="14">
    <if_group>sysmon_event1</if_group>
    <field name="win.eventdata.image" type="pcre2">(?i)\\mshta\.exe$</field>
    <field name="win.eventdata.commandLine" type="pcre2">(?i)(https?|ftp|\\\\|vbscript|javascript)</field>
    <description>LOLBin: mshta выполняет удалённый контент - $(win.eventdata.commandLine)</description>
    <mitre><id>T1218.005</id></mitre>
  </rule>
```

Рисунок 3 – Правило корреляции

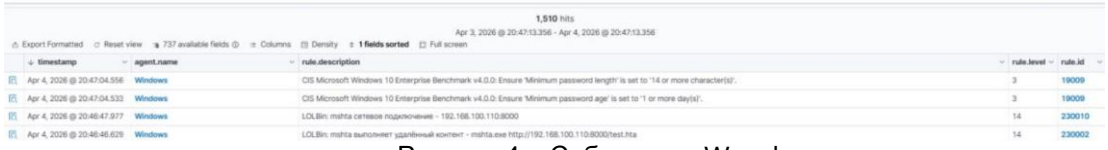


Рисунок 4 – События на Wazuh

Таким образом, можно сделать вывод о том, что регулярное написание правил корреляции крайне необходимо для повышения киберустойчивости информационной системы. Также, необходимо учитывать, что злоумышленники могут использовать легитимные утилиты для своих целей.

***Список использованных источников:***

*1. LoLBins [Электронный ресурс]. – Режим доступа: https://www.securitylab.ru/glossary/lolbins/ – Дата доступа: 03.04.2026.*

*2. Как подготовиться к LotL- атакам на [Электронный ресурс]. – Режим доступа: https://www.kaspersky.co.uk/blog/lotl-attacks-detection-hardening-guidance/27389/ – Дата доступа: 03.04.2026.*

*3. Cybercriminals' top LoLBins [Электронный ресурс]. – Режим доступа: https://www.kaspersky.com/blog/most-used-lolbins/42180/ – Дата доступа: 03.04.2026.*

*4. The Open Source Security Platform [Электронный ресурс]. – Режим доступа: https://wazuh.com/ – Дата доступа: 03.04.2026.*

*5. One unified platform for complete protection [Электронный ресурс]. – Режим доступа: https://wazuh.com/platform/overview/ – Дата доступа: 03.04.2026.*

*6. mshta.exe [Электронный ресурс]. – Режим доступа: https://www.reviversoft.com/ru/processes/mshta.exe?ncr=1 – Дата доступа: 03.04.2026*

*7. Why do adversaries use Mshta? [Электронный ресурс]. – Режим доступа: https://redcanary.com/threat-detection-report/techniques/mshta/ – Дата доступа: 03.04.2026.*

*8. System Binary Proxy [Электронный ресурс]. – Режим доступа: https://attack.mitre.org/techniques/T1218/005/ – Дата доступа: 03.04.2026.*

*9. Rules Syntax [Электронный ресурс]. – Режим доступа: https://documentation.wazuh.com/current/user-manual/ruleset/ruleset-xml-syntax/rules.html – Дата доступа: 03.04.2026.*

*10. Regular Expression Syntax [Электронный ресурс]. – Режим доступа: https://documentation.wazuh.com/current/user-manual/ruleset/ruleset-xml-syntax/regex.html – Дата доступа: 03.04.2026.*

*11. Sysmon версии 15.2 [Электронный ресурс]. – Режим доступа: https://learn.microsoft.com/ru-ru/sysinternals/downloads/sysmon – Дата доступа: 03.04.2026.*