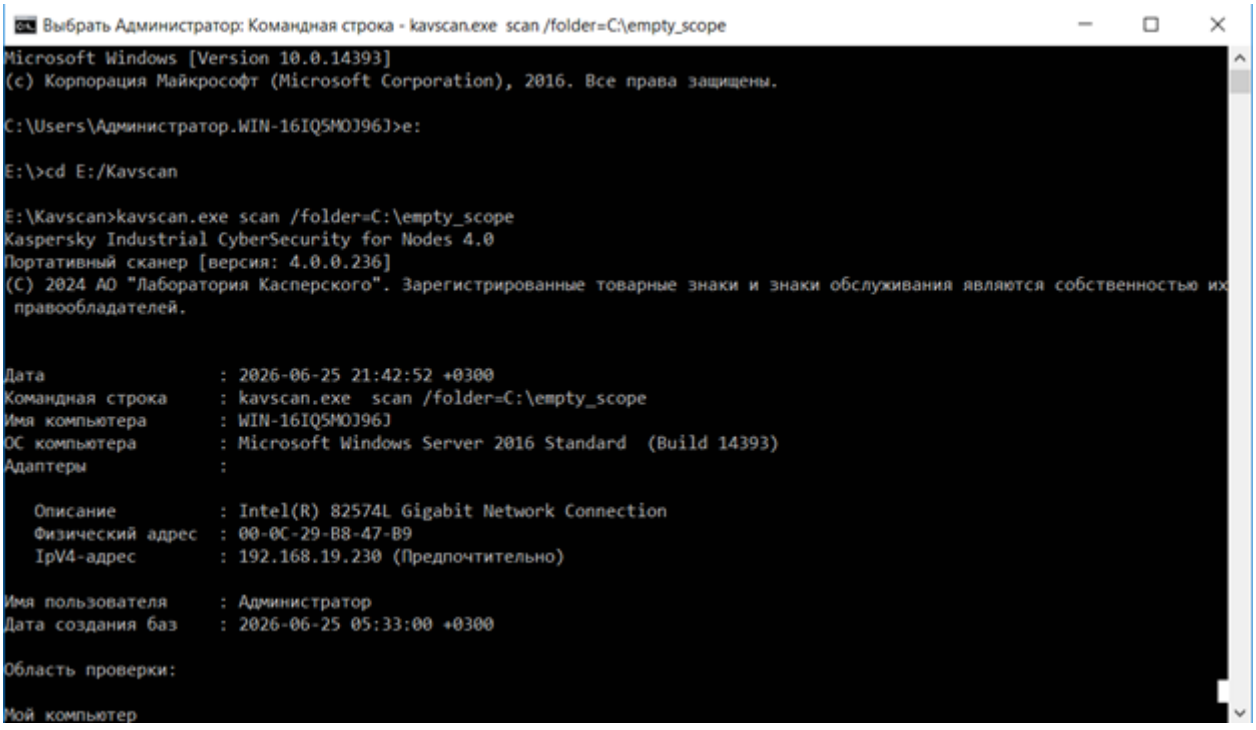
?????????????? ?????????????? ??????? (v4.0) ??????? ???????? ? ???? ?????????

? ???? ?????? ??????????? ???????? ???????? ?????????? ???????????? ???????. ??? ?????? ?????? ? ???????? ?????????? ????????? ???????????????? ????????:

1. ????????? ????????? ?????? ? ??????? ?????????????? ? ????????? ??????? ?? ????, ?? ??????? ?????????? ?????? (????????, e:).
2. ????????? ? ??????? ???????: cd E:/Kavscan.
3. ??? ?????? ??????? ????????????? ????????? ???????? ??????? ???????? ??? ???????? ???????? ???????. ??? ???????? ???????????????? ??????: ????? ??????????? ? ???????????? ? ?????? ???????????? ?????????, ?????????? ?? ????? ???????? ????????. ?? ??????????? ??????? ???????????? ?????? ????????? ?? ????????? (?? ??????????? ??????? ?????????? ???).



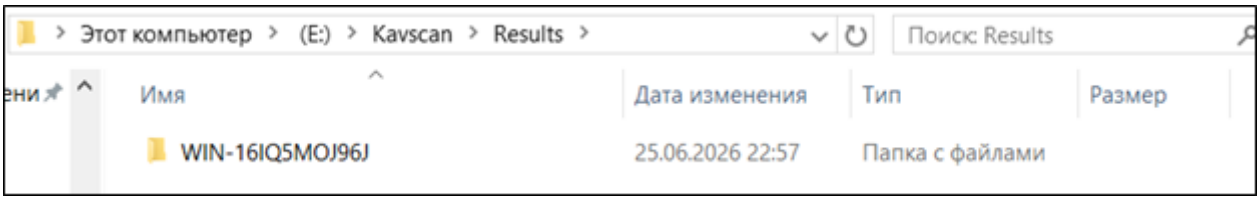
????????? ????? ??????? ????? ????????????:

```
E:\Kavscan>kavscan.exe export /folder=E:\Kavscan\Results /clean
Kaspersky Industrial CyberSecurity for Nodes 4.0
Портативный сканер [версия: 4.0.0.236]
(C) 2024 АО "Лаборатория Касперского". Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их
 правообладателей.


Дата                : 2026-06-25 22:43:25 +0300
Командная строка    : kavscan.exe  export /folder=E:\Kavscan\Results /clean
Имя компьютера      : WIN-16IQ5MOJ96J
ОС компьютера       : Microsoft Windows Server 2016 Standard  (Build 14393)
Адаптеры            :

   Описание         : Intel(R) 82574L Gigabit Network Connection
   Физический адрес : 00-0C-29-B8-47-B9
   IpV4-адрес       : 192.168.19.230 (Предпочтительно)

Имя пользователя    : Администратор

Экспорт результатов в папку E:\Kavscan\Results...
```

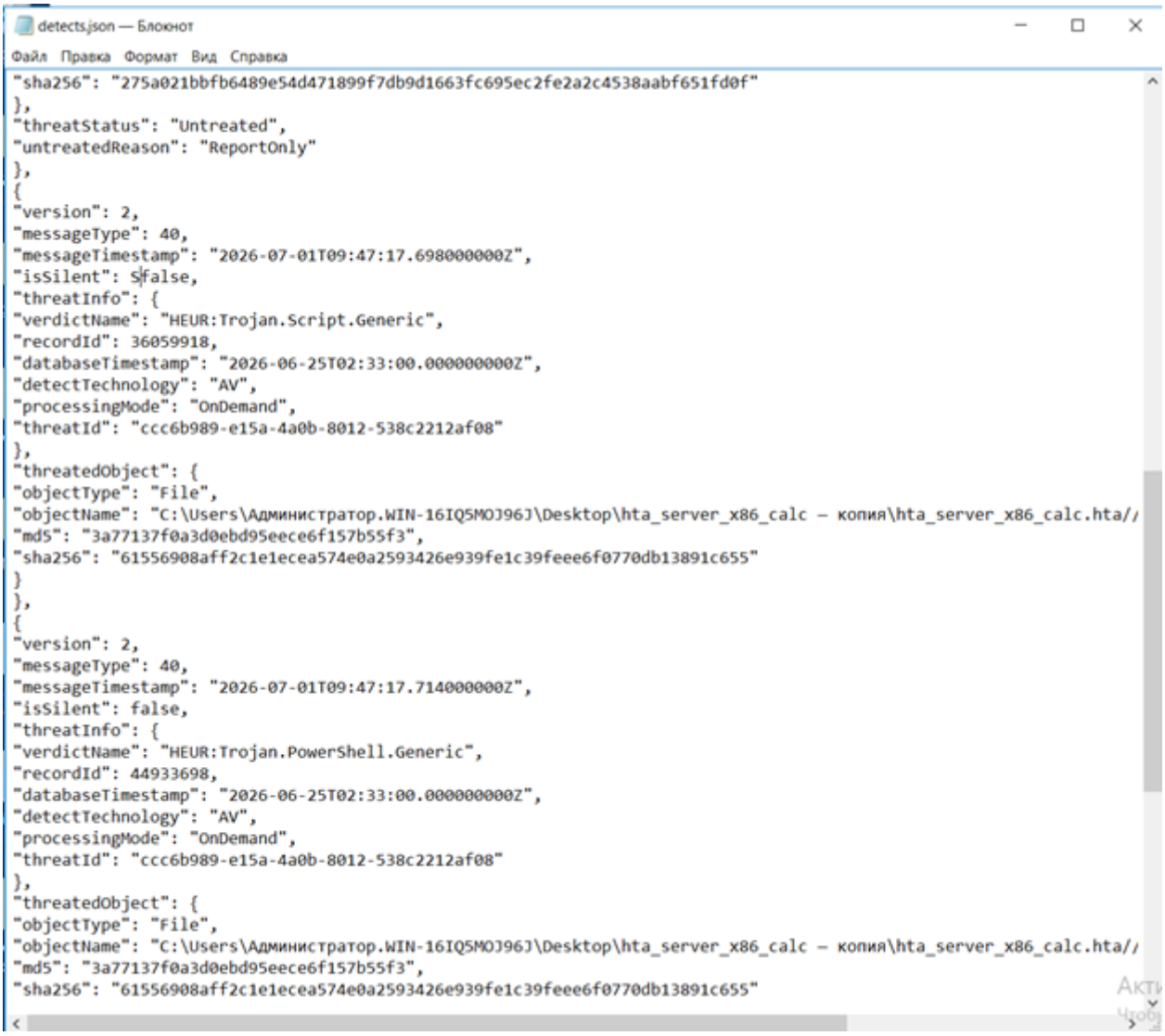
?????? ????????? ????????????????? ? ?????? ??????????? ? ????????????? ??????????.

```
E:\Kavscan>kavscan.exe scan /av
Kaspersky Industrial CyberSecurity for Nodes 4.0
Портативный сканер [версия: 4.0.0.236]
(C) 2024 АО "Лаборатория Касперского". Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.


Дата                : 2026-07-01 12:44:41 +0300
Командная строка    : kavscan.exe  scan /av
Имя компьютера      : WIN-16IQ5MOJ96J
ОС компьютера       : Microsoft Windows Server 2016 Standard  (Build 14393)
Адаптеры            :

   Описание         : Intel(R) 82574L Gigabit Network Connection
   Физический адрес : 00-0C-29-B8-47-B9
   IpV4-адрес       : 192.168.19.230 (Предпочтительно)

Имя пользователя    : Администратор
Дата создания баз   : 2026-06-25 05:33:00 +0300

Область проверки:

Мой компьютер


Сканирование завершено

Сканирование началось в 2026-07-01 12:44:54 +0300
Сканирование завершилось в 2026-07-01 13:22:18 +0300

Статистика:

Обнаружено: 1
Зараженных и других обнаруживаемых объектов: 1
Возможно зараженных объектов: 4
Не вылечено объектов: 0
Не удалено объектов: 0
Не проверено объектов: 80
Объектов, не помещенных в резервное хранилище: 0
Ошибок обработки: 0
Вылечено объектов: 0
Помещено в резервное хранилище: 0
Удалено объектов: 0
Защищенных паролем объектов: 3
Зашифрованных объектов: 0
Обработано объектов: 405853
```

?? ?????? ???????????? ???? ???????? ??????????, ? ????? ???????????? ?????????? ???????. ?????????? ????????? ??????? ?????????? ??????????.
? ??????????? ???????, ??????????? ?? ???????????? USB-??????????, ??? ?????? ??????????? ? ???????? Kavscan\Result. ?????? ????? ???????? ??? ??????? ???????????? ?????????? ????????? ????????? ?????, ? ??????? ????? ?????????? ????????? ??????? — ? ??????????? ?? ????, ??????? ??? ??????????? ???????????? ??????? ????.



?????????????? ?????? — ???????? ?????? ?????, ???????????? ?????????? ????????. ??? ????? ?????????? ??????? ???? detects.json, ??????? ???????? ?????? ???????? ?????????? ???????? ? ????????? ?? ??????? ? ??????????????.



???????????? ??????????? ????? ???????????? ????? ????????? ??????, ??? ??? ????? ????????? ??????????? ???, ??? ????? ????????? ?? ???????????? ?????. ??????? ?????? ????? ?????????? ??????????????? ? ???????????????? ??.

????????, ?????????? ???????????? ?????? `hta_server_x86_calc.hta`.

?????? ???? ???????? ??? ?????? ??????:

- **HEUR:Trojan.Script.Generic**: ??? ????????????? ??????????? ??????????? ???????. ?????? ????? ???? ????????????? ??? ?????????? ??????????????? ???????? ?? ???????, ????? ??? ????????, ??????????, ????????? ??? ??????????? ??????. ??????? ?????? ??????????? ??? **???????**.

- **HEUR:Trojan.PowerShell.Generic**: ??? ????????????? ??????????? ???????????? ???????, ????????????? PowerShell. ????? ?????? ????? ??????????? ??? ???????? ? ?????????? ????????????? ??????????? ??????????? ?? ?????????.

?????? "threatStatus": "Untreated" ? ???????? "untreatedReason": "ReportOnly" ????????, ??? ?????? **?????????, ?? ?? ?????? ? ?? ???????? ? ????????** ?????????? ????. ??? ??????????? ????????? ??? ???????????? ??????? KICS, ??????? ???????? ? ?????? «?????? ???????????» (Report Only). ??? ???????? ?????? — ??????? ?????? ??? ???????????? ???????, ? ?? ????????????? ???????.

??? ??? ?????? ?? ???? ????????????? ?????????, ?????????? ??????????? ????????? ????:

1. **??????????? ?????????? ????**: ????????? ????????? ?? ???????????? ???? ??? ????????????? ????????????? ?????. ???? ?????????? ?? ????????????? ?????????, ?? ?????????, ??? ????? ?? ????????????? ?? ?????? ???????. ????????? ???????????? ?????? ??????????? ????????.
2. **??????? ?????????? ????**: ??????? ??????? ???? hta_server_x86_calc.hta ? ???????? ?????.
3. **???????? ?????? ????????????**: ????????? ?????? ???????????? ???? ??????? ? ??????? ???????????? ??????? ??? ????????? ????????????? ???????, ????? ????????? ? ?????????? ?????? ?????????? ????????.
4. **??????????????? ??????? ?????????**: ????????, ??? ???? ????? ?? ?????????. ??? ????? ???? ?????????? ???????, ???????? ? ???????????? ????? ??? ????????????? ????? ?????? ????????.
5. **????????? ??????? ??????????**: ???????????????? ??????? ?????????? ? ??????????? ???? ??? ????????? ????????? ?????? ?????? ??? ????? ? ????????-???????????? (C2) ?????????.

??? ??????? ?????, ?????????? ??????????? ???????? KICS, ????? ???????????? ????????? ????? ?????????. ??? ???????????? ?? ??????????: ???? ??????? ?????? ??????? ??????, ?????? — ???????? ???????? ????????????? ?????????.

??????? ?????????? ????????? ?????????:

Kaspersky Threat Intelligence: ????????? «??????????? ???????????» ????????????? ?????????? ?????? ?? ???-???????, ????? ??????, ????????? ????? ? ????????????? ???????. (https://opentip.kaspersky.com/)

????????????? ?????? (ICS CERT): «??????????? ???????????» ????????? ???????? ??????????? ?????? ? ??????????? ?? ???????????? ???????????. (https://ics-cert.kaspersky.com/)

???? ????? ???????????? ? ??????????? ?? «??????????? ???????????» (https://threats.kaspersky.com/ru/)

irusTotal: ??????-??????, ??????? ????????? ???? ??? ??? (SHA256/MD5) ????????? ???????????? ??????? ? ?????????? ?????????? ?? ???? ????????. ??? ????????? ???????, ????????? ?????? ???? ????????????? ??? ??????????? (https://www.virustotal.com/gui/home/upload).

Revision #1
Created 9 July 2026 11:41:24 by Olga Sinotova
Updated 9 July 2026 11:55:41 by Olga Sinotova