

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

- **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>).