19 / 54

Community Score 98

19/54 security vendors flagged this file as malicious

Reanalyze Similar More

fab408536aa37c4abc8be97ab9c1f86cb33b63923d423fdc2…

QbotUninstall.exe

pedll idle checks-user-input

Size 11.00 KB

Last Analysis Date 3 months ago

DLL

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 5

Voting details (3)

SolarSciencePup 1 year ago +1	**Artilllerie** 1 year ago +39	**jameswt** 1 year ago +58

Comments (2)

thor
1 year ago

YARA Signature Match - THOR APT Scanner

RULE: SUSP_QakBot_Uninstaller_FBI_Aug23
RULE_SET: Livehunt - Suspicious183 Indicators 🏹
RULE_TYPE: THOR APT Scanner's rule set only 🔨
RULE_LINK: https://valhalla.nextron-systems.com/info/rule/SUSP_QakBot_Uninstaller_FBI_Aug23
DESCRIPTION: Detects Qakbot uninstaller used by the FBI / Dutch Police
REFERENCE: https://www.justice.gov/usao-cdca/divisions/national-security-division/qakbot-resources
RULE_AUTHOR: Florian Roth

Show more

mgraeber_rc
1 year ago

Extracted PE from published FBI QBot takedown shellcode:
https://www.virustotal.com/gui/file/7cdee5a583eacf24b1f142413aabb4e556ccf4ef3a4764ad084c1526cc90e117

You must be **signed in** to post a comment.

Sign in

Sign up