

1

/ 63

Community Score

175

1/63 security vendor flagged this file as malicious

Reanalyze

Similar

More

7cdee5a583eacf24b1f142413aabb4e556ccf4ef3a4764ad084c1526cc90e117

Size

Last Analysis Date

fbi\_7cde

13.54 KB

3 months ago







DETECTION

DETAILS











COMMUNITY20+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.


Contained in Graphs (3)

 kic_937	Copy of Qbot uninstall binary	2023-08-31 09:23:47	
 kic_937	Qbot uninstall binary	2023-08-31 09:21:53	
 FEVAR54	ACTIVIDAD MALICIOSA   Relacionada con Qakbot 30-08-2023	2023-08-30 15:36:15	

Voting details (12)

 <b>PeteXT</b> 1 year ago +1	 <b>SolarSciencePup</b> 1 year ago +1	 <b>Quemandoacromo</b> 1 year ago +34
 <b>ventaran</b> 1 year ago +1	 <b>Artillerie</b> 1 year ago +39	 <b>Malware_Enjoyer</b> 1 year ago +1
 <b>ice_wzl</b> 1 year ago +1	 <b>CrocodylII</b> 1 year ago +1	 <b>Omnicide</b> 1 year ago +1
 <b>OleMadhatter</b> 1 year ago +1		

Comments (7)

 **JaffaCakes118**  
1 year ago

File Info:

Filename:  
DB92062F94839DC8F0E94EF6C14B113A



Threat Score:  
1/10

Family:


We use cookies and related technologies to remember user preferences, for security, to analyse our traffic, and to enable website functionality. Learn more about cookies in our [Privacy Notice](#).

Ok






[Sign in](#)[Sign up](#)

 1 year ago



*Qbot/QakBot uninstaller by FBI and CISA*  
> <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-242a>

#Pinkslipbot #TA570 #GoldLagoon



**thor**  
 1 year ago






YARA Signature Match - THOR APT Scanner

RULE: SUSP\_Qakbot\_Uninstaller\_File\_Aug23  
RULE\_SET: Livehunt - Suspicious158 Indicators   
RULE\_TYPE: THOR APT Scanner's rule set only   
RULE\_LINK: [https://valhalla.nexttron-systems.com/info/rule/SUSP\\_Qakbot\\_Uninstaller\\_File\\_Aug23](https://valhalla.nexttron-systems.com/info/rule/SUSP_Qakbot_Uninstaller_File_Aug23)  
DESCRIPTION: Detects Qakbot Uninstaller files used by the FBI and Dutch National Police in a disruption operation against the Qakbot in August 2023  
REFERENCE: <https://www.justice.gov/usao-cdca/divisions/national-security-division/qakbot-resources>  
RULE\_AUTHOR: Florian Roth  
[Show more](#)




**patricksvgapi**  
 1 year ago



This indicator was mentioned in a report.

-  Title: Identification and Disruption of QakBot Infrastructure
-  Reference: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-242a>
-  Report Publish Date: 2023-08-29
-  Sample Upload Date: 2023-08-29
-  Reference ID: #00c649fb8 (<https://www.virustotal.com/gui/search/00c649fb8/comments> for report's related indicators)




**thor**  
 1 year ago

YARA Signature Match - THOR APT Scanner


RULE: SUSP\_Qakbot\_Uninstaller\_File  
RULE\_SET: Livehunt - Suspicious179 Indicators   
RULE\_TYPE: THOR APT Scanner's rule set only   
RULE\_LINK: [https://valhalla.nexttron-systems.com/info/rule/SUSP\\_Qakbot\\_Uninstaller\\_File](https://valhalla.nexttron-systems.com/info/rule/SUSP_Qakbot_Uninstaller_File)  
DESCRIPTION: Detects Qakbot Uninstaller files used by the FBI and Dutch National Police in a disruption operation against the Qakbot in August 2023  
REFERENCE: <https://www.justice.gov/usao-cdca/divisions/national-security-division/qakbot-resources>  
RULE\_AUTHOR: Florian Roth  
[Show more](#)



**mgraeber\_rc**  
 1 year ago

x86 shellcode that decrypts and executes the following EXE:  
<https://www.virustotal.com/gui/file/fab408536aa37c4abc8be97ab9c1f86cb33b63923d423fdc2859eb9d63fa8ea0>



**victor\_rocheron**  
 1 year ago

FBI uninstaller for QBOT Takedown  
Find sha256 mentionned here : <https://www.justice.gov/usao-cdca/divisions/national-security-division/qakbot-resources>

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

We use cookies and related technologies to remember user preferences, for security, to analyse our traffic, and to enable website functionality. Learn more about cookies in our [Privacy Notice](#).

Ok

Our product	Community	Tools	Premium Services	Documentation
<a href="#">Contact Us</a>	<a href="#">Join Community</a>	<a href="#">API Scripts</a>	<a href="#">Get a demo</a>	<a href="#">Searching</a>
<a href="#">Get Support</a>	<a href="#">Vote and Comment</a>	<a href="#">YARA</a>	<a href="#">Intelligence</a>	<a href="#">Reports</a>
<a href="#">How It Works</a>	<a href="#">Contributors</a>	<a href="#">Desktop Apps</a>	<a href="#">Hunting</a>	<a href="#">API v3   v2</a>
<a href="#">ToS   Privacy Notice</a>	<a href="#">Top Users</a>	<a href="#">Browser Extensions</a>	<a href="#">Graph</a>	<a href="#">Use Cases</a>
<a href="#">Blog   Releases</a>	<a href="#">Community Buzz</a>	<a href="#">Mobile App</a>	<a href="#">API v3   v2</a>	