



Settings



Post



Omri Segev Moyal 
@GelosSnake



Another example: [app.anyrun.run/tasks/3cb68f0c...](https://anyrun.run/tasks/3cb68f0c...)

ADVANCED DETAILS OF PROCESS

20

out of 100

No verdict

Download

svchost.exe (id: 3880)

CA\Users\admin\AppData\Local\Temp\7zZNE97HE7\svchost.exe

Parent process: a25a8fde2b06ca71a175ccf5543b39f14017698c72709ef2bb5da1d63cb0a4bf.exe (id: 3408)

User: admin

SID: S-1-5-21-1302019708-1500728564-335382590-1000

IL: MEDIUM

Timeline

Created 0 +640

Terminated 60 Was run

Children

No children

Look up on VT

Command Line:

C:\Users\admin\AppData\Local\Temp\7zZNE97HE7\svchost.exe -o stratum+tcp://fcn-xmr.pool.minergate.com:45590 -u alexanderotherlione1@live.com -p x -k -B --cpu-priority 0 --date-level 1

Version Information:

Company: Microsoft Corporation

Description: Host Process for Windows Services

Version: 10.0.10240.16384 (th1.150709-1700)

INDICATORS OF SUSPICIOUS BEHAVIOUR

10:44 PM · Nov 26, 2017

8 Likes



Don't miss what's happening
People on X are the first to know.

Log in

Sign up

Welcome to x.com!



We are letting you know that we are changing our URL, but your privacy and data protection settings remain the same.
For more details, see our Privacy Policy: <https://x.com/en/privacy>.

Did someone say ... cookies?

X and its partners use cookies to provide you with a better, safer and faster service and to support our business. Some cookies are necessary to use our services, improve our services, and make sure they work properly. [Show more about your choices.](#)

Accept all cookies

Refuse non-essential cookies