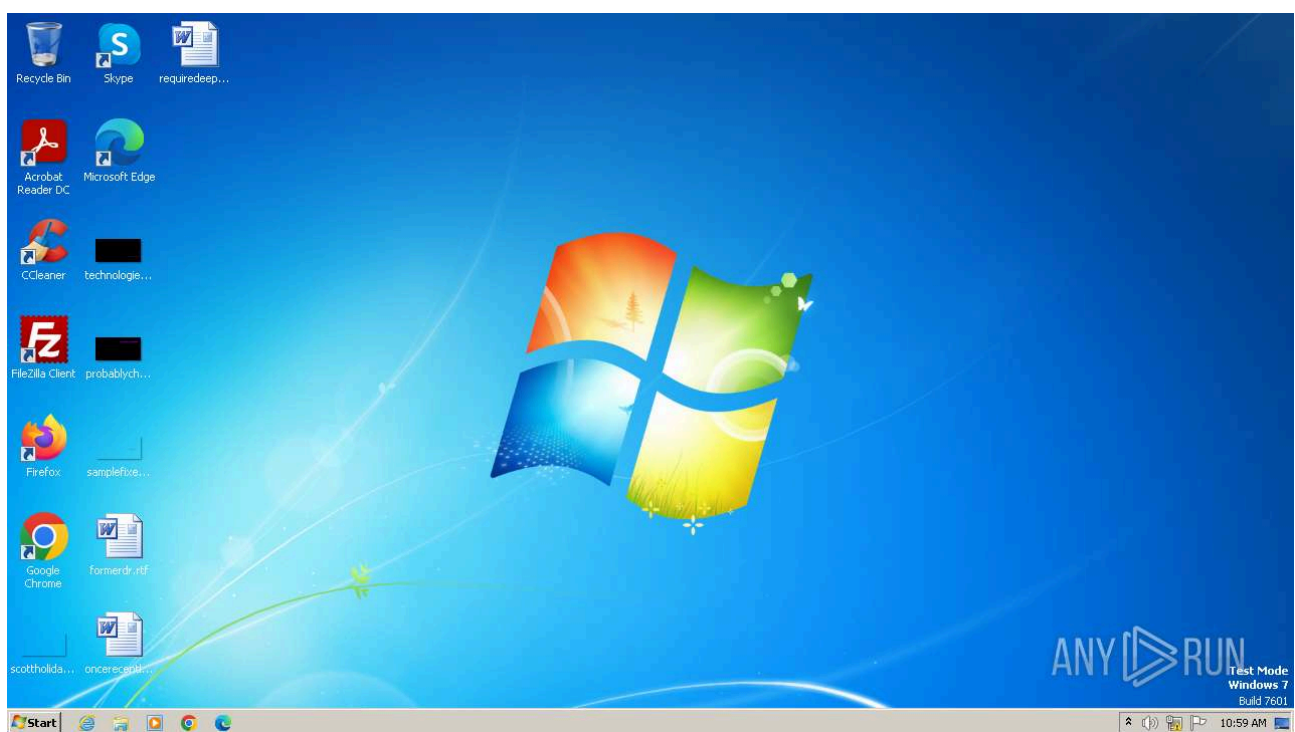


Analysis KSA-PDA_17122023.exe (MD5: 3DFF19E34ED9A7F7CCC7D64000884890) Malicious activity - Interactive analysis ANY.RUN

Archived: 2026-04-05 21:46:32 UTC



Move your mouse to view screenshots



Hide whitelisted

Timeshift

Headers

Rep

PID

Process name

CN

URL

Content

- 18437 ms

H1

GET 200: OK

3972

KSA-PDA_17122023.exe

<http://checkip.dyndns.org/>

106 b

html

- 18440 ms

H1

GET 200: OK

3972

KSA-PDA_17122023.exe

<http://checkip.dyndns.org/>

106 b

html

- 19429 ms

H1

GET 200: OK

3972

KSA-PDA_17122023.exe

<http://checkip.dyndns.org/>

106 b

html

- 19430 ms

H1

GET 200: OK

3972

KSA-PDA_17122023.exe

<http://checkip.dyndns.org/>

106 b

html

- 20428 ms

H1

GET 200: OK

3972

KSA-PDA_17122023.exe

<http://checkip.dyndns.org/>

106 b

html

- 20429 ms

H1

GET 200: OK

3972

KSA-PDA_17122023.exe

<http://checkip.dyndns.org/>

106 b

html

- 20431 ms

H1

GET 200: OK

3972

KSA-PDA_17122023.exe

http://checkip.dyndns.org/

106 b

html

- 20432 ms

H1

GET 200: OK

3972

KSA-PDA_17122023.exe

http://checkip.dyndns.org/

106 b

html

- 21446 ms

H1

GET 200: OK

3972

KSA-PDA_17122023.exe

http://checkip.dyndns.org/

106 b

html

 Malicious activity

KSA-PDA_17122023.exe

MD5:

3dff19e34ed9a7f7ccc7d64000884890

Start:

06.06.2024, 09:59

Total time:

57 s

[Text report](#)



Save time with new AI Summaries

Get a quick understanding of malicious behavior thanks to actionable AI insights.

CPU

RAM

-

- beta

Only important

3972

KSA-PDA_17122023.exe

DMP

gaboongrabber



1k



5k



78

4056

wmpnscfg.exe



17



13



8

Source: <https://app.any.run/tasks/65855217-7209-4eae-a572-b030a2305b22/>