


The screenshot displays the ANY.RUN web-based remote execution platform. The top section shows a virtualized Windows XP desktop with various icons like Recycle Bin, Firefox, FileZilla Client, Google Chrome, Opera, Skype, CCleaner, VLC media player, and several PDF files. A large white text overlay reads "MOVE YOUR MOUSE TO VIEW SCREENSHOTS" with a mouse cursor icon below it. The bottom section features a dark blue sidebar with navigation links: "+ New analysis", "Reports", "TI", "Pricing", "Contacts", "FAQ", and "Sign In". To the right of the sidebar is a table summarizing system activity:



Win7 32 bit

Complete

64uc1




MD5: 6EFD45B1FDDE7E292FC089B8038685E3

Start: 01.10.2019, 15:21    Total time: 300 s

emotet

trojan

Indicators:

Tracker: [Emotet](#), [Trojan](#)

Get sample

IOC

MalConf

Restart

Text report

Graph

ATT&CK

Summary beta

Export

CPU

RAM

Processes

Filter by PID or name

Only important

3468

64uc1.exe

PE

232

0

64

976

64uc1.exe

PE

-977a3569

emotet

406

45

84

3580

msptermisizes.exe

PE

174

0

62

2452

msptermisizes.exe

PE

-f91b2738

emotet

494

30

112

2696

o0ZysJD.exe

PE

150

0

62

3632

o0ZysJD.exe

PE

-975bd459

emotet

408

24

86

4056

msptermisizes.exe

PE

174

0

62

2728

msptermisizes.exe

PE

-f91b2738

emotet

312

18

by PID, name or url

PCAP

Content

46

82

49

14

Try community version for free!

Register now