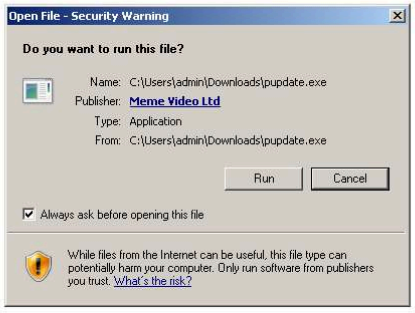
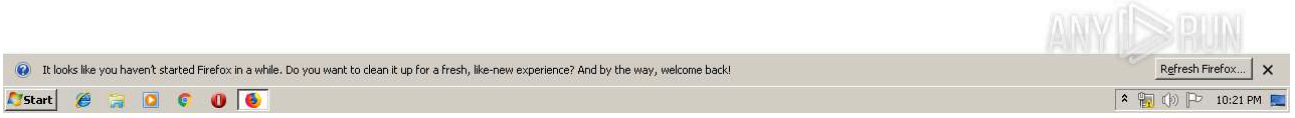
Analysis http://getapp.normandoh.com/up/dl/1514720375122642/pupdate.exe Malicious activity - Interactive analysis ANY.RUN

Archived: 2026-04-05 12:46:45 UTC

Move your mouse to view screenshots





-
-
-

Timeshift

Headers

Rep

PID

Process name

CN

URL

Content

http://getapp.normandoh.com/up/dl/1514720375122642/pupdate.exe

Start:

19.07.2019, 21:20

Total time:

58 s

-
-

Lost connection with guest OS while task running

3868

firefox.exe

"http://getapp.normandoh.com/up/dl/1514720375122642/pupdate.exe"

2616

firefox.exe

-contentproc --channel="3868.0.1919910712\3527278" -parentBuildID 20190619235627 -greomni "C:\Program Files\Mozilla Firefox\omni.ja" -appomni "C:\Program Files\Mozilla Firefox\browser\omni.ja" -appdir "C:\Program Files\Mozilla Firefox\browser" - 3868 "\\.\pipe\gecko-crash-server-pipe.3868" 1168 gpu

4000

firefox.exe

-contentproc --channel="3868.3.1233738814\1074657126" -childID 1 -isForBrowser -prefsHandle 1640 -prefMapHandle 1636 -prefsLen 1 -prefMapSize 188076 -parentBuildID 20190619235627 -greomni "C:\Program Files\Mozilla Firefox\omni.ja" -appomni "C:\Program Files\Mozilla Firefox\browser\omni.ja" -appdir "C:\Program Files\Mozilla Firefox\browser" - 3868 "\\.\pipe\gecko-crash-server-pipe.3868" 1320 tab

3504

firefox.exe

-contentproc --channel="3868.13.1673596704\1166091922" -childID 2 -isForBrowser -prefsHandle 2708 -prefMapHandle 2712 -prefsLen 5842 -prefMapSize 188076 -parentBuildID 20190619235627 -greomni "C:\Program Files\Mozilla Firefox\omni.ja" -appomni "C:\Program Files\Mozilla Firefox\browser\omni.ja" -appdir "C:\Program Files\Mozilla Firefox\browser" - 3868 "\\.\pipe\gecko-crash-server-pipe.3868" 2716 tab

3484

firefox.exe

-contentproc --channel="3868.20.1447472350\216281834" -childID 3 -isForBrowser -prefsHandle 3624 -prefMapHandle 3628 -prefsLen 6604 -prefMapSize 188076 -parentBuildID 20190619235627 -greomni "C:\Program Files\Mozilla Firefox\omni.ja" -appomni "C:\Program Files\Mozilla Firefox\browser\omni.ja" -appdir "C:\Program Files\Mozilla Firefox\browser" - 3868 "\\.\pipe\gecko-crash-server-pipe.3868" 3720 tab

3060

schtasks.exe

/create /SC DAILY /TN ZUpdater /TR "\"C:\Users\admin\AppData\Roaming\ZUpdater\ZUpdater.exe\" do://zupdater

3728

pingsender.exe

https://incoming.telemetry.mozilla.org/submit/telemetry/4a8d22c5-e560-429e-aa1a-6c71020553e4/event/Firefox/67.0.4/release/20190619235627?v=4 C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\qldyz51w.default\saved-telemetry-pings\4a8d22c5-e560-429e-aa1a-6c71020553e4

3344

pingsender.exe

https://incoming.telemetry.mozilla.org/submit/telemetry/931f1892-26d7-4ed3-b578-fc43eda2e515/health/Firefox/67.0.4/release/20190619235627?v=4 C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\qldyz51w.default\saved-telemetry-pings\931f1892-26d7-4ed3-b578-fc43eda2e515

3700

pingsender.exe

https://incoming.telemetry.mozilla.org/submit/telemetry/5402ddc0-4435-4423-baa8-fb54f6be43c6/main/Firefox/67.0.4/release/20190619235627?v=4 C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\qldyz51w.default\saved-telemetry-pings\5402ddc0-4435-4423-baa8-fb54f6be43c6
