Sandbox Report

File: bruno_1.30.0_x64_win.exe

Resubmit | Print | Download options

SHA-256
b89b17bda73aadd...41158d3e62af69

Submitted by
dhruv.kaith@fisglobal.com

Discovered

Detonation environment
Windows 11 64, Professional, 10.0 (build 22621)

Network settings
Network connectivity turned off

Timestamp
Sep. 26, 2024 21:05:10

Threat level
Malicious

Threat score
100/100

Tags
Evasive

Static analysis | Dynamic analysis | Intelligence | MITRE ATT&CK

Behavioral threat indicators

Malicious

4

Spawns a lot of processes

Source	Monitored Target
Relevance	8/10
MITRE ATT&CK	Process Discovery T1057
Details	Spawned process "bruno_1.30.0_x64_win.exe" (UID: 00000000-00007128) Spawned process "cmd.exe" with commandline "cmd /c tasklist /FI "USERNAME eq %USERNAME%" /FI "IMAGENAME eq Bruno.exe" | find "Bruno.exe"" (UID: 00000000-00005152) Spawned process "tasklist.exe" with commandline "tasklist /FI "USERNAME eq %OSUSER%" /FI "IMAGENAME eq Bruno.exe"" (UID: 00000000-00003600) Spawned process "find.exe" with commandline "find "Bruno.exe"" (UID: 00000000-00004528) Spawned process "Bruno.exe" (UID: 00000000-00003184) Spawned process "Bruno.exe" with commandline ""%APPDATA%\\bruno" --gpu-preferences=WAAAAAAAAADgAAAMAAAAAAAAAAAAAAAAAABgAAEAAAA4AAAAAAAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGAAAAAAAAAAYAAAAAAAAAAgAAAAAAAAACAAAAAAAAAAIAAAAAAAAAA== --field-trial-handle=1780,i,15614198459324415054,5951785769167937056,262144 --disable-features=SpareRendererForSitePerProcess,WinDelaySpellcheckServiceInit,WinRetrieveSuggestionsOnlyOnDemand --variations-seed-version --mojo-platform-channel-handle=1772 /prefetch:2" (UID: 00000000-00009428) Spawned process "Bruno.exe" with commandline ""%APPDATA%\\bruno" --field-trial-handle=3032,i,15614198459324415054,5951785769167937056,262144 --disable-

Writes data to a remote process

Source API Call

Relevance 6/10

MITRE ATT&CK Process Injection T1055

Details

"C:\Users\%OSUSER%\AppData\Local\Programs\bruno\Bruno.exe" (Handle: 2924) "Bruno.exe" wrote 00000004 bytes to a remote process
"C:\Users\%OSUSER%\AppData\Local\Programs\bruno\Bruno.exe" (Handle: 2924) "Bruno.exe" wrote 000011C0 bytes to a remote process
"C:\Users\%OSUSER%\AppData\Local\Programs\bruno\Bruno.exe" (Handle: 3028) "Bruno.exe" wrote 00000008 bytes to a remote process
"C:\Users\%OSUSER%\AppData\Local\Programs\bruno\Bruno.exe" (Handle: 3028) "Bruno.exe" wrote 000011C0 bytes to a remote process
"C:\Users\%OSUSER%\AppData\Local\Programs\bruno\Bruno.exe" (Handle: 2588) "Bruno.exe" wrote 00000008 bytes to a remote process
"C:\Users\%OSUSER%\AppData\Local\Programs\bruno\Bruno.exe" (Handle: 2588) "Bruno.exe" wrote 000011C0 bytes to a remote process
"C:\Users\%OSUSER%\AppData\Local\Programs\bruno\Bruno.exe" (Handle: 3100) "Bruno.exe" wrote 00000008 bytes to a remote process
"C:\Users\%OSUSER%\AppData\Local\Programs\bruno\Bruno.exe" (Handle: 3100) "Bruno.exe" wrote 00000068 bytes to a remote process
"C:\Users\%OSUSER%\AppData\Local\Programs\bruno\Bruno.exe" (Handle: 3100) "Bruno.exe" wrote 00000020 bytes to a remote process
"C:\Users\%OSUSER%\AppData\Local\Programs\bruno\Bruno.exe" (Handle: 3100) "Bruno.exe" wrote 00000010 bytes to a remote process
"C:\Users\%OSUSER%\AppData\Local\Programs\bruno\Bruno.exe" (Handle: 3100)

Changes memory access rights in a remote process to write/execute

Source API Call

Relevance 3/10

MITRE ATT&CK Process Injection T1055

Details "Bruno.exe" changed protection rights in "C:\Users\%OSUSER%\AppData\Local\Programs\bruno\Bruno.exe" (Handle: 2924) (Protection: "write-copy") "Bruno.exe" changed protection rights in "C:\Users\%OSUSER%\AppData\Local\Programs\bruno\Bruno.exe" (Handle: 2924) (Protection: "execute/read") "Bruno.exe" changed protection rights in "C:\Users\%OSUSER%\AppData\Local\Programs\bruno\Bruno.exe" (Handle: 3100) (Protection: "write-copy") "Bruno.exe" changed protection rights in "C:\Users\%OSUSER%\AppData\Local\Programs\bruno\Bruno.exe" (Handle: 3100) (Protection: "execute/read")

Tries to gather information about running processes on a system

Source Monitored Target

Relevance 3/10

MITRE ATT&CK Process Discovery T1057

Details Process "tasklist.exe" with commandline "tasklist /FI "USERNAME eq %OSUSER%" /FI "IMAGENAME eq Bruno.exe"" (UID: 00000000-00003600)

Suspicious 51

Informative 186

Process details

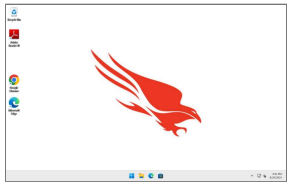
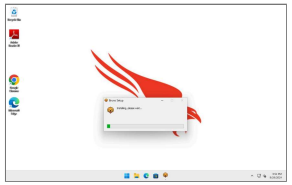
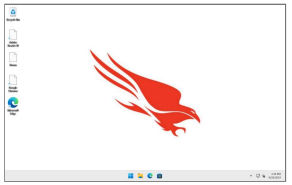
- bruno_1.30.0_x64_win.exe PID 7128
  - cmd.exe PID 5152
    - tasklist.exe PID 3600
    - find.exe PID 4528
- Bruno.exe PID 3184
  - Bruno.exe PID 9428
  - Bruno.exe PID 3340
  - Bruno.exe PID 9912
  - Bruno.exe PID 9480
  - Bruno.exe PID 9476
  - Bruno.exe PID 9036
  - Bruno.exe PID 2588
  - Bruno.exe PID 9460

Bruno.exe PID 9064

Bruno.exe PID 9580

Bruno.exe PID 8592

Screenshots

Discovered URL analysis

No verdict 1

Extracted strings

Download extracted strings

bruno_1.30.0_x64_win.exe 552

nsExec.dll 1

WinShell.dll	1
Bruno.exe	203
cmd.exe	26
tasklist.exe	21
Bruno.lnk	1
LICENSE.electron.txt	1
app-update.yml	1

Extracted files

No verdict	23