VIRUSTOTAL

SUMMARY DETECTION DETAILS RELATIONS BEHAVIOR

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

Display grouped sandbox reports

CAPE Sandbox	⚠ 0	3	0	0	54	10
VirusTotal Juju…	⚠ 0	0	0	0	0	0
Zenbox	⚠ 0	6	0	0	47	0

Activity Summary

Download Artifacts Full Reports Help

⚠ Detections
NOT FOUND

Mitre Signatures
22 INFO

IDS Rules
NOT FOUND

Sigma Rules
NOT FOUND

Dropped Files
8 OTHER 1 PE_EXE 1 TEXT

Network comms

5 DNS 5 IP

Behavior Tags

checks-user-input detect-debug-environment long-sleeps

MITRE ATT&CK Tactics and Techniques

- Persistence TA0003
- Privilege Escalation TA0004
- Defense Evasion TA0005
- Credential Access TA0006
- Discovery TA0007
- Collection TA0009
- Command and Control TA0011

Network Communication

DNS Resolutions

+ business.bing.com
+ bzib.nelreports.net
  edge-consumer-static.azureedge.net
+ edge-mobile-static.azureedge.net
  edgeassetservice.azureedge.net

IP Traffic

TCP 204.79.197.203:443
TCP 209.85.200.94:443
TCP 13.107.253.70:443 (edge-mobile-static.azureedge.net)
TCP 13.107.6.158:443 (business.bing.com)
TCP 104.98.118.170:443 (bzib.nelreports.net)

Memory Pattern Domains

darkbasicpro.thegamecreators.com
darkphysics.thegamecreators.com
forum.thegamecreators.com
github.com
www.thegamecreators.com

Memory Pattern Urls

http://darkbasicpro.thegamecreators.com
http://darkbasicpro.thegamecreators.com/?f=dark_ai
http://darkbasicpro.thegamecreators.com/?f=dark_lights
http://darkbasicpro.thegamecreators.com/?f=darkclouds
http://darkbasicpro.thegamecreators.com/?f=darkink
http://darkbasicpro.thegamecreators.com/?f=darkkfs
http://darkbasicpro.thegamecreators.com/?f=darknet
http://darkbasicpro.thegamecreators.com/?f=enhanced_animations
http://darkbasicpro.thegamecreators.com/?f=enhancementpack
http://darkbasicpro.thegamecreators.com/?f=extends

Behavior Similarity Hashes

CAPE Sandb…	7463e911a17119efabd77aa8c27be64f
VirusTotal Ju…	9fcbde393f2f22333f9bedd64dba31ce
Zenbox	2bd48b636e6f97cbb422b0b50347b6be

File system actions

Files Opened

- C:\ProgramData\Microsoft\
- C:\ProgramData\Microsoft\Windows\
- C:\ProgramData\Microsoft\Windows\WER
- C:\ProgramData\Microsoft\Windows\WER\
- C:\ProgramData\Microsoft\Windows\WER\ReportArchive
- C:\ProgramData\Microsoft\Windows\WER\ReportArchive\27d9c2bb-c050-4667-a6d3-bd1aad90aba6
- C:\ProgramData\Microsoft\Windows\WER\ReportArchive\5cef414b-5c9b-4cf2-9dc0-4e65237092a9
- C:\ProgramData\Microsoft\Windows\WER\ReportArchive\e1bd7946-908c-4c5c-9442-4a8f73bd322c
- C:\ProgramData\Microsoft\Windows\WER\ReportQueue
- C:\ProgramData\Microsoft\Windows\WER\ReportQueue\805fd7c9-2990-4009-a332-3553f4aa8ca6

Files Written

- C:\ProgramData\Microsoft\Windows\WER\ReportArchive
- C:\ProgramData\Microsoft\Windows\WER\ReportArchive\27d9c2bb-c050-4667-a6d3-bd1aad90aba6
- C:\ProgramData\Microsoft\Windows\WER\ReportArchive\5cef414b-5c9b-4cf2-9dc0-4e65237092a9
- C:\ProgramData\Microsoft\Windows\WER\ReportArchive\e1bd7946-908c-4c5c-9442-4a8f73bd322c
- C:\ProgramData\Microsoft\Windows\WER\ReportQueue
- C:\ProgramData\Microsoft\Windows\WER\ReportQueue\805fd7c9-2990-4009-a332-3553f4aa8ca6
- C:\ProgramData\Microsoft\Windows\WER\ReportQueue\963fe01c-24f6-403b-a978-1bf30cf824f0
- C:\ProgramData\Microsoft\Windows\WER\ReportQueue\a23490e5-adc8-489e-9254-43346d01b0c6
- C:\ProgramData\Microsoft\Windows\WER\Temp
- C:\ProgramData\Microsoft\Windows\WER\Temp\00d8f706-40c4-486e-b87c-7df9d4cd900b

Files Deleted

- C:\ProgramData\Microsoft\Windows\WER\Temp\WER9338.tmp

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9338.tmp.dmp
C:\ProgramData\Microsoft\Windows\WER\Temp\WER985A.tmp
C:\ProgramData\Microsoft\Windows\WER\Temp\WER985A.tmp.WERInterr
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9ABC.tmp.xml
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB5AA.tmp
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB5AA.tmp.dmp
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB9B2.tmp
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB9B2.tmp.WERInterr

Files Dropped

+ DBPro9Ex_v1009/DBPro9Ex_20170604/Changelog.txt
+ DBPro9Ex_v1009/DBPro9Ex_20170604/Compiler/DBPCompiler.exe
+ DBPro9Ex_v1009/DBPro9Ex_20170604/Compiler/Precompiler/StringLiterals.dl
+ DBPro9Ex_v1009/DBPro9Ex_20170604/Compiler/Precompiler/bin/include/Line
+ DBPro9Ex_v1009/DBPro9Ex_20170604/Compiler/Precompiler/bin/include/Pre
+ DBPro9Ex_v1009/DBPro9Ex_20170604/Compiler/Precompiler/bin/include/Pro
+ DBPro9Ex_v1009/DBPro9Ex_20170604/Compiler/Precompiler/bin/include/Sou
+ DBPro9Ex_v1009/DBPro9Ex_20170604/Compiler/Precompiler/bin/lib/Precomp Library.lib
+ DBPro9Ex_v1009/DBPro9Ex_20170604/Compiler/lang/english/Errors.txt
+ DBPro9Ex_v1009/DBPro9Ex_20170604/Compiler/plugins-licensed/DBProGameFX.dll

Registry actions

Registry Keys Opened

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\E Folders\Cache
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Tl
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Tl
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Windows Error Reporting\AutoApproveOSDumps
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Windows Error Reporting\BypassDataThrottling

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Windows Error Reporting\BypassNetworkCostThrottling
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Windows Error Reporting\BypassPowerThrottling
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Windows Error Reporting\Consent
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Windows Error Reporting\DebugApplications

Process and service actions

Processes Created

- "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" "C:\Use <USER>\AppData\Local\Temp\DBPro9Ex_v1009/DBPro9Ex_20170604/Hel MULTITHREADED DIRECTX.html"
- "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" "C:\Use <USER>\AppData\Local\Temp\DBPro9Ex_v1009/DBPro9Ex_20170604/Hel VIRTUAL TEXTURE MANAGEMENT.html"
- "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" "C:\Use <USER>\AppData\Local\Temp\DBPro9Ex_v1009/DBPro9Ex_20170604/Hel VIRTUAL TEXTURE MANAGEMENT.html"
- "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" "C:\Use <USER>\AppData\Local\Temp\DBPro9Ex_v1009/DBPro9Ex_20170604/Hel VIRTUAL TEXTURE MANAGEMENT ENABLED.html"
- "C:\Users\ <USER>\AppData\Local\Temp\DBPro9Ex_v1009/DBPro9Ex_20170604/Cor
- "C:\Windows\system32\rundll32.exe" "C:\Users\ <USER>\AppData\Local\Temp\DBPro9Ex_v1009/DBPro9Ex_20170604/Cor
- "C:\Windows\system32\rundll32.exe" "C:\Users\ <USER>\AppData\Local\Temp\DBPro9Ex_v1009/DBPro9Ex_20170604/Cor licensed/DBProGameFX.dll",#1
- "C:\Windows\system32\rundll32.exe" "C:\Users\ <USER>\AppData\Local\Temp\DBPro9Ex_v1009/DBPro9Ex_20170604/Cor user/SC_Collision.dll",#1
- "C:\Windows\system32\rundll32.exe" "C:\Users\ <USER>\AppData\Local\Temp\DBPro9Ex_v1009/DBPro9Ex_20170604/Cor
- "C:\Windows\system32\rundll32.exe" "C:\Users\ <USER>\AppData\Local\Temp\DBPro9Ex_v1009/DBPro9Ex_20170604/Cor

Shell Commands

"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=c handler "--user-data-dir=C:\Users\<USER>\AppData\Local\Microsoft\Edge Data" /prefetch:4 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\<USER>\AppData\Local\Microsoft\Edge\User Data\Cra annotation=IsOfficialBuild=1 --annotation=channel= --annotation=chromi version=122.0.6261.129 "--annotation=exe=C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --annotation=plat=Win64 " annotation=prod=Microsoft Edge" --annotation=ver=122.0.2365.92 --initia data=0x32c,0x330,0x334,0x328,0x33c,0x7ffc34615fd8,0x7ffc34615fe4,0x7f

"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=g preferences=WAAAAAAAAADgAAAMAAAAAAAAAAAAAAAAAABgAAAAAAA4AA --mojo-platform-channel-handle=2136 --field-trial-handle=2140,i,9058462

"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --no-appcompat-clear --mojo-platform-channel-handle=2404 --field-trial-handle=2140,i,9058462584944229435,8825304115337877520,262144 --variations-seed-version /prefetch:3

C:\Windows\SysWOW64\WerFault.exe -u -p 1556 -s 744

C:\Windows\SysWOW64\WerFault.exe -u -p 1948 -s 724

C:\Windows\SysWOW64\WerFault.exe -u -p 6076 -s 704

Processes Terminated

C:\Users\user\AppData\Local\Temp\3hwrvfsl.cxo\DBPro9Ex_v1009\DBPrc

C:\Windows\SysWOW64\7za.exe

C:\Windows\SysWOW64\cmd.exe

C:\Windows\SysWOW64\unarchiver.exe

Processes Tree

5932 - "C:\Users\<USER>\AppData\Local\Temp\DBPro9Ex_v1009/DBPro9Ex_20170604/Compil

2960 - "C:\Windows\system32\rundll32.exe" "C:\Users\<USER>\AppData\Local\Temp\DBPro9Ex_v1009/DBPro9Ex_20170604/Compil

3376 - "C:\Windows\system32\rundll32.exe" "C:\Users\<USER>\AppData\Local\Temp\DBPro9Ex_v1009/DBPro9Ex_20170604/Compil

2988 - "C:\Windows\system32\rundll32.exe" "C:\Users\<USER>\AppData\Local\Temp\DBPro9Ex_v1009/DBPro9Ex_20170604/Compil

2212 - "C:\Windows\system32\rundll32.exe" "C:\Users\<USER>\AppData\Local\Temp\DBPro9Ex_v1009/DBPro9Ex_20170604/Compil

3808 - "C:\Windows\system32\rundll32.exe" "C:\Users\<USER>\AppData\Local\Temp\DBPro9Ex_v1009/DBPro9Ex_20170604/Compil

4116 - "C:\Windows\system32\rundll32.exe" "C:\Users\<USER>\AppData\Local\Temp\DBPro9Ex_v1009/DBPro9Ex_20170604/Compil

3004 - "C:\Windows\system32\rundll32.exe" "C:\Users\<USER>\AppData\Local\Temp\DBPro9Ex_v1009/DBPro9Ex_20170604/Compil

1276 - "C:\Windows\system32\rundll32.exe" "C:\Users\<USER>\AppData\Local\Temp\DBPro9Ex_v1009/DBPro9Ex_20170604/Compil

4636 - "C:\Windows\system32\rundll32.exe" "C:\Users\<USER>\AppData\Local\Temp\DBPro9Ex_v1009/DBPro9Ex_20170604/Compil

Synchronization mechanisms & Signals

Mutexes Created

- Global\AmiProviderMutex_InventoryApplicationFile
- Global\b5c72e12-7eb4-4171-8150-272f982e203e
- Global\c08e41f3-af68-476f-af3e-ffd1ac24aeda
- Global\d8d502b3-027e-4a87-9b7b-655e58d5a7e9
- Local\WERReportingForProcess1556
- Local\WERReportingForProcess1948
- Local\WERReportingForProcess6076

Modules loaded

Runtime Modules

- NTDLL.DLL

Highlighted actions

Calls Highlighted

- NtResumeProcess
- NtSuspendProcess
- GetTickCount

Highlighted Text

- "Optional update delivery is not working"