xcitium

PUA
Xcitium Final Verdict

File Name: Pro.Evolution.Soccer.20GamingBeasts.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: bca71c098aadb35a4e94f1f68d239eab1d11f52a
MD5: c350eacfe1e1e28295eb961af91e70f8
First Seen Date: 2023-05-26 10:40:32 UTC
Number of Clients Seen: 13
Last Analysis Date: 2023-06-06 08:02:14 UTC
Human Expert Analysis Date: 2023-06-06 08:02:13 UTC
Human Expert Analysis Result: PUA
Verdict Source: Xcitium Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2023-06-06 08:02:14 UTC	Clean
Static Analysis Overall Verdict	2023-06-02 04:29:16 UTC	No Threat Found
Precise Detectors Overall Verdict	2023-06-06 08:02:14 UTC	No Match
Human Expert Analysis Overall Verdict	2023-06-06 08:02:13 UTC	PUA
File Certificate Validation		Vendor not found in Trusted List

Static Analysis

STATIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

DETECTOR	RESULT
Optional Header LoaderFlags field is valued illegal	Clean
Non-ascii or empty section names detected	Clean
Illegal size of optional Header	Clean
Packer detection on signature database	Unknown
Based on the sections entropy check! file is possibly packed	Suspicious
Timestamp value suspicious	Clean
Header Checksum is zero!	Clean
Enrty point is outside the 1st(.code) section! Binary is possibly packed	Clean
Optional Header NumberOfRvaAndSizes field is valued illegal	Clean
Anti-vm present	Clean
The Size Of Raw data is valued illegal! Binary might crash your disassembler/debugger	Clean
TLS callback functions array detected	Clean

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

SUSPICIOUS BEHAVIORS	
Uses a function clandestinely	!
Has no visible windows	!

Behavioral Information

LoadLibrary

ADVAPI32.dll

QueryProcessAddress

CreateProcessW
ShellExecuteW

QueryFilePath

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Static Precise PUA Detector 1	2023-06-03 21:35:23 UTC	No Match	?	NotDetected
Static Precise PUA Detector 4	2023-06-03 21:35:23 UTC	No Match	?	NotDetected
Static Precise NI Detector 3	2023-06-03 21:35:23 UTC	No Match	?	NotDetected
Static Precise PUA Detector 5	2023-06-03 21:35:23 UTC	No Match	?	NotDetected
Static Precise Trojan Detector 1	2023-06-03 21:35:23 UTC	No Match	?	NotDetected
Static Precise Trojan Detector 3	2023-06-03 21:35:23 UTC	No Match	?	NotDetected
Static Precise PUA Detector 6	2023-06-03 21:35:23 UTC	No Match	?	NotDetected
Static Precise Trojan Detector 12	2023-06-03 21:35:23 UTC	No Match	?	NotDetected
Static Precise Virus Detector 1	2023-06-03 21:35:23 UTC	No Match	?	NotDetected
Static Precise Virus Detector 2	2023-06-03 21:35:23 UTC	No Match	?	NotDetected
Static Precise Trojan Detector 13	2023-06-03 21:35:23 UTC	No Match	?	NotDetected
Static Precise PUA Detector 2	2023-06-03 21:35:23 UTC	No Match	?	NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2023-05-26 12:40:29 UTC
Analysis End Date: 2023-06-06 08:02:13 UTC
File Upload Date: 2023-05-26 10:40:00 UTC
Human Expert Analyst Feedback:
Verdict: PUA
Malware Family: Application
Malware Type: Pua

Additional File Information

Vendor Validation - Not Verified ✖

[+] SOFTWARE ABFG LTD

Status	Not Valid ✖

Certificate Validation - Success ✔

[+] GlobalSign Code Signing Root R45

Status	NoError ✔
Start Date	2020-03-18 02:00:00
End Date	2045-03-18 02:00:00
Sha256	b8baa24483dd03798b6b593aad05d12bea93e069693742f53008d28a7bb95e92
Serial	7653FEAC75464893F5E5D74A483A4EF8
Subject Name	GlobalSign Code Signing Root R45
Subject Key Identifier	1f 00 bf 46 80 0a fc 78 39 b7 a5 b4 43 d9 56 50 bb ce 96 3b
Subject Organization	GlobalSign nv-sa
Subject Country	BE
Issuer Name	GlobalSign Code Signing Root R45
Issuer Key Identifier	null
Issuer Organization	GlobalSign nv-sa
Issuer Country	BE
Crl link	null
Key Usage	{"Digital Signature","Certificate Signing","Off-line CRL Signing","CRL Signing (86)"}
Extended Usage	null

[+] GlobalSign Code Signing Root R45

Status	NoError ✔
Start Date	2020-03-18 02:00:00
End Date	2045-03-18 02:00:00
Sha256	b8baa24483dd03798b6b593aad05d12bea93e069693742f53008d28a7bb95e92
Serial	7653FEAC75464893F5E5D74A483A4EF8
Subject Name	GlobalSign Code Signing Root R45
Subject Key Identifier	1f 00 bf 46 80 0a fc 78 39 b7 a5 b4 43 d9 56 50 bb ce 96 3b
Subject Organization	GlobalSign nv-sa
Subject Country	BE
Issuer Name	GlobalSign Code Signing Root R45
Issuer Key Identifier	null
Issuer Organization	GlobalSign nv-sa
Issuer Country	BE
Crl link	null
Key Usage	{"Digital Signature","Certificate Signing","Off-line CRL Signing","CRL Signing (86)"}
Extended Usage	null

[+] GlobalSign GCC R45 EV CodeSigning CA 2020

Status	NoError ✔
Start Date	2020-07-28 03:00:00
End Date	2030-07-28 03:00:00
Sha256	a71858b369d4729065cdc3b96a65aed3ef6b031fe7caf3b0955d4207fbb82703
Serial	77BD0E05B7590BB61D4761531E3F75ED
Subject Name	GlobalSign GCC R45 EV CodeSigning CA 2020
Subject Key Identifier	25 9d d0 fc 59 09 86 63 c5 ec f3 b1 13 3b 57 1c 03 92 36 11
Subject Organization	GlobalSign nv-sa
Subject Country	BE
Issuer Name	GlobalSign Code Signing Root R45
Issuer Key Identifier	1f 00 bf 46 80 0a fc 78 39 b7 a5 b4 43 d9 56 50 bb ce 96 3b
Issuer Organization	GlobalSign nv-sa
Issuer Country	BE
Crl link	http://crl.globalsign.com/codesigningrootr45.crl
Key Usage	{"Digital Signature","Certificate Signing","Off-line CRL Signing","CRL Signing (86)"}
Extended Usage	{"Code Signing (1.3.6.1.5.5.7.3.3)"}

[+] SOFTWARE ABFG LTD

Status	RevocationStatusUnknown ✖
Start Date	2023-03-22 04:10:47
End Date	2024-03-22 04:10:47
Sha256	7cd66fc699072d2576bc11707032b9e33867aa531cb7e2a1946aef5100325b15
Serial	3C22F5C916B284010CB8A481
Subject Name	SOFTWARE ABFG LTD
Subject Key Identifier	3c 5b a8 96 b2 8b ae 07 df d4 4d ec a6 2b 7a f5 f1 4c bd c6
Subject Organization	SOFTWARE ABFG LTD
Subject Locality	Ruislip
Subject State	London
Subject Country	GB
Issuer Name	GlobalSign GCC R45 EV CodeSigning CA 2020
Issuer Key Identifier	25 9d d0 fc 59 09 86 63 c5 ec f3 b1 13 3b 57 1c 03 92 36 11
Issuer Organization	GlobalSign nv-sa
Issuer Country	BE
Crl link	http://crl.globalsign.com/gsgccr45evcodesignca2020.crl
Key Usage	{"Digital Signature (80)"}
Extended Usage	{"Code Signing (1.3.6.1.5.5.7.3.3)"}

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x646F17DC [Thu May 25 08:10:04 2023 UTC]
Debug Artifacts	
Entry Point	0x4024f2 (.text)
Exifinfo	
File Size	203120
File Type Enum	6
Imphash	
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Mime Type	application/x-dosexec
Number Of Sections	5
Sha256	0b0dbc8833cc08b6d44607278f7945b015c23dcfd2531cd5fe38b5dc65d28f5b
Ssdeep	
Trid	

File Paths

FILE PATH ON CLIENT	SEEN COUNT
C:\Users\ibrahim.gormez\Downloads\Your File Is Ready To Download.exe	5
C:\Users\serkan.dinc\Downloads\Your File Is Ready To Download.exe	5
C:\Users\kdiaz\Downloads\Your File Is Ready To Download (1).exe	5
C:\Users\aba.kantar\Downloads\Your File Is Ready To Download.exe	5
C:\Users\sumit_it\Downloads\Pro.Evolution.Soccer.20GamingBeasts.exe	5

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x9ca4	0x9e00	6.54365017831	7954e3edf71628ed362680d37db68c4b
.rdata	0xb000	0x1e7e	0x2000	5.3451273928	90319f4515606c625cccdb03e4b0f2ca
.data	0xd000	0xf79c	0xda00	7.6567456283	853aaeeebf0369a3acc1e4fe84be9c6f
.rsrc	0x1d000	0x13d8c	0x13e00	3.90850559206	9c9f4cc955168ffffb42b32331e85d41
.reloc	0x31000	0x1192	0x1200	4.34444312919	09f6b0bc7ff674a66c6feefbace7fb46