VALKYRIE

CLEAN
Valkyrie Final Verdict

File Name: d161035af5e273586f836bb7bbe1f221bdefb508Erp.UI.PkgControlConfirmPCIDEntry.dll
File Type: PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
SHA1: d161035af5e273586f836bb7bbe1f221bdefb508
MD5: 7614b0bd804a546ab10edb0928a5ca80
First Seen Date: 2020-02-14 04:55:03 UTC
Number of Clients Seen: 10
Last Analysis Date: 2021-01-14 17:18:03 UTC
Human Expert Analysis Date: 2020-02-17 15:50:50 UTC
Human Expert Analysis Result: Clean
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2021-01-14 17:18:03 UTC	Clean	✓
Static Analysis Overall Verdict	2021-01-14 17:18:03 UTC	No Threat Found	?
Precise Detectors Overall Verdict	2021-01-14 17:18:03 UTC	No Match	?
Human Expert Analysis Overall Verdict	2020-02-17 15:50:50 UTC	Clean	✓
File Certificate Validation		Not Applicable	?

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	Clean	✓
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	✓

Packer detection on signature database

Microsoft Visual C# / Basic .NET

Dynamic Analysis

No Dynamic Analysis Result Received

Behavioral Information is not Available

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Static Precise PUA Detector 1	2021-01-14 17:18:00 UTC	No Match		NotDetected
Static Precise PUA Detector 4	2021-01-14 17:18:00 UTC	No Match		NotDetected
Static Precise NI Detector 3	2021-01-14 17:18:00 UTC	No Match		NotDetected
Static Precise PUA Detector 5	2021-01-14 17:18:00 UTC	No Match		NotDetected
Static Precise Trojan Detector 1	2021-01-14 17:18:00 UTC	No Match		NotDetected
Static Precise Trojan Detector 3	2021-01-14 17:18:00 UTC	No Match		NotDetected
Static Precise PUA Detector 6	2021-01-14 17:18:00 UTC	No Match		NotDetected
Static Precise Trojan Detector 12	2021-01-14 17:18:00 UTC	No Match		NotDetected
Static Precise Virus Detector 1	2021-01-14 17:18:00 UTC	No Match		NotDetected
Static Precise Virus Detector 2	2021-01-14 17:18:00 UTC	No Match		NotDetected
Static Precise Trojan Detector 13	2021-01-14 17:18:00 UTC	No Match		NotDetected
Static Precise PUA Detector 2	2021-01-14 17:18:00 UTC	No Match		NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2020-02-17 11:46:33 UTC
Analysis End Date: 2020-02-17 15:50:50 UTC
File Upload Date: 2020-02-17 09:03:08 UTC
Human Expert Analyst Feedback: None
Verdict: Clean

Additional File Information

Vendor Validation - Vendor Validation is not Applicable ?

Certificate Validation - Certificate Validation is not Applicable ?

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x5CA7053E [Fri Apr 5 07:35:26 2019 UTC]
Debug Artifacts	[object Object]
Entry Point	0x110089be (.text)
Exifinfo	[object Object]
File Size	40960
File Type Enum	6
Imphash	dae02f32a21e03ce65412f6e56942daa
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	22
Translation	0x0000 0x04b0
Legal Copyright	(c) 2003-2019 Epicor Software Corporation: All Rights Reserved
Assembly Version	10.2.400.0
Internal Name	Erp.UI.PkgControlConfirmPCIDEntry.dll
File Version	10.2.400.0
Company Name	Epicor
Comments	
Product Name	Epicor Application
Product Version	10.2.400.0
File Description	
Original Filename	Erp.UI.PkgControlConfirmPCIDEntry.dll
Mime Type	application/x-dosexec
Number Of Sections	3
Sha256	1addc75115c630ac0e6fd4f0102e83948e756cc9c40f57f06427ad3c763f0c08
Ssdeep	768:SpergNVH3Q/ztZFWGIgJOEhHLFIKcZJLalnA:SpergNVHcZ8GIgnhRIKc7N
Trid	38.3,Win32 Dynamic Link Library (generic),26.2,Win32 Executable (generic),12,Win16/32 Executable Delphi generic,11.6,Generic Win/DOS Executable,11.6,DOS Executable Generic

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x2000	0x69c4	0x7000	5.39215566326	ad029ee72dc9b1e690d431cd5aceddb3
.rsrc	0xa000	0x430	0x1000	1.10740594547	ddd9d032a4172f7b1a669485ec22e518
.reloc	0xc000	0xc	0x1000	0.0131269437212	b4884109d1c4cf68dd56be006eaec034