



File Name: IVeckQArv.342

File Type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

SHA1: 4a573351cf0dfe6f27ef3f2ad46547907974596f **MD5:** c7b49ae21e22eab80c938e4a74d1bea6 **First Seen Date:** 2016-12-26 15:20:13 UTC

Number of Clients Seen: 4

Last Analysis Date: 2016-12-26 15:20:13 UTC

Human Expert Analysis Date: 2016-12-27 06:23:00 UTC

Human Expert Analysis Result: Malware

Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

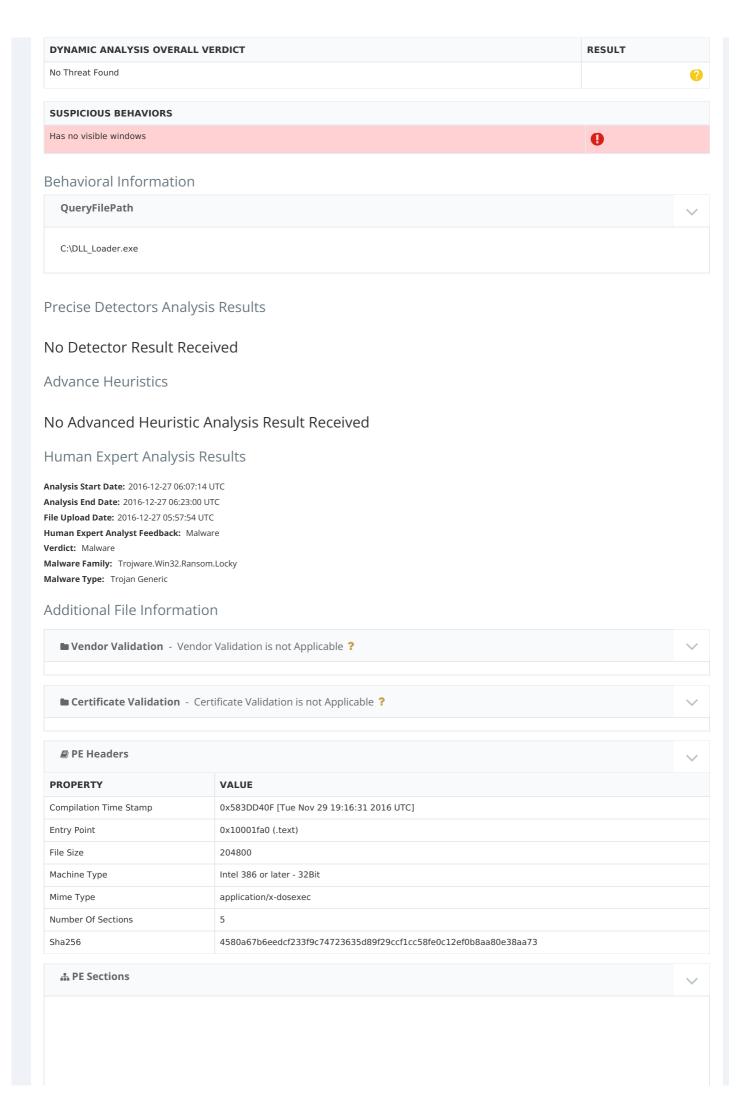
ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2016-12-26 15:20:13 UTC	Malware	0
Static Analysis Overall Verdict	2016-12-26 15:20:13 UTC	No Threat Found	?
Dynamic Analysis Overall Verdict	2016-12-26 15:20:13 UTC	No Threat Found	?
Human Expert Analysis Overall Verdict	2016-12-27 06:23:00 UTC	Malware	0
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	Ø
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	②
Header Checksum is zero!	Suspicious	0
Enrty point is outside the 1st(.code) section! Binary is possibly packed	Clean	②
Optional Header NumberOfRvaAndSizes field is valued illegal	Clean	©
Anti-vm present	Clean	②
The Size Of Raw data is valued illegal! Binary might crash your disassembler/debugger	Clean	•
TLS callback functions array detected	Clean	Ø

Dynamic Analysis



NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x6dde	0×7000	5.972678	-
.rdata	0x8000	0x13fe	0x2000	3.463543	-
.data	0xa000	0x2634c	0x26000	5.504609	-
.rsrc	0x31000	0xa0	0×1000	0.096823[SUSPICIOUS]	-
.reloc	0x32000	0xb9a	0×1000	5.075811	-
≛ PE Im	ports				~
- &	msi.dll				
- &	KERNEL32.dll				
	VirtualAlloc				
-	MSVCRT.dll				
	allonexit				
	memcpy				
	onexit				
	malloc malloc malloc malloc				
	adjust_fdiv				
♣ PE Ex	ports				~
₹?Se	rtData@@YGXXZ				
□ DE Do	sources				

ⓓ RT_STRING