VALKYRIE

CLEAN
Valkyrie Final Verdict

File Name: dccrap.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
SHA1: 98a29905d9ccc3c3ab9b58ba1cce7daf41ae91c0
MD5: 2ddf4fe039e7562f6256c3ade57b2b98
First Seen Date: 2016-04-19 11:15:51 UTC
Number of Clients Seen: 6
Last Analysis Date: 2018-11-29 00:47:00 UTC
Human Expert Analysis Result: No human expert analysis verdict given to this sample yet.
Verdict Source: Signature Based Detection

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2018-11-29 00:46:53 UTC	Clean	✓
Static Analysis Overall Verdict	2018-11-29 00:47:00 UTC	No Threat Found	?
Precise Detectors Overall Verdict	2018-11-29 00:47:00 UTC	No Match	?
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	Suspicious	!
Timestamp value suspicious	Suspicious	!
Header Checksum is zero!	Suspicious	!
Enrty point is outside the 1st(.code) section! Binary is possibly packed	Suspicious	!
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

📦 UPX 2.90 [LZMA] -> Markus Oberhumer, Laszlo Molnar & John Reiser

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	2018-11-29 00:46:55 UTC	No Match	❓	NotDetected
Static Precise Trojan Detector 5	2018-11-29 00:46:55 UTC	No Match	❓	NotDetected
Static Precise Trojan Detector 7	2018-11-29 00:46:55 UTC	No Match	❓	NotDetected
Static Precise PUA Detector 4	2018-11-29 00:46:55 UTC	No Match	❓	NotDetected
Static Precise PUA Detector 5	2018-11-29 00:46:55 UTC	No Match	❓	NotDetected
Static Precise Trojan Detector 1	2018-11-29 00:46:55 UTC	No Match	❓	NotDetected
Static Precise Trojan Detector 2	2018-11-29 00:46:55 UTC	No Match	❓	NotDetected
Static Precise Trojan Detector 3	2018-11-29 00:46:55 UTC	No Match	❓	NotDetected
Static Precise Trojan Detector 12	2018-11-29 00:46:55 UTC	No Match	❓	NotDetected
Static Precise Trojan Detector 10	2018-11-29 00:46:55 UTC	No Match	❓	NotDetected
Static Precise Virus Detector 1	2018-11-29 00:46:56 UTC	No Match	❓	NotDetected
Static Precise Virus Detector 2	2018-11-29 00:46:56 UTC	No Match	❓	NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Additional File Information

🖿 **Vendor Validation** - Vendor Validation is not Applicable ❓   ⌄

🖿 **Certificate Validation** - Certificate Validation is not Applicable ❓   ⌄

🗐 **PE Headers**   ⌄

PROPERTY	VALUE
Compilation Time Stamp	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC] [SUSPICIOUS]
Debug Artifacts	
Entry Point	0x1062960 (UPX1)
Exifinfo	[object Object]
File Size	3029504
File Type Enum	6
Imphash	01bac83367b70d09fc0b1b02e8890c9b
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Legal Copyright	
Internal Name	DC-Unlocker Client
File Version	1.0.4.60
Company Name	UAB Digiteka
Legal Trademarks	
Comments	http://www.dc-unlocker.com
Product Name	DataCard-Unlocker Client
Product Version	1.0.0.0
File Description	Data Card Unlocker client software
Original Filename	dc-unlocker2client.exe
Translation	0x0809 0x04e4
Mime Type	application/x-dosexec
Number Of Sections	3
Sha256	9437de5e2601f8155646e83ee0878f1d625b6edaa007d0203f62e6be94a230ea
Ssdeep	49152:RrF24Pjtm6IXDpzk3f0mlBirtcvGQCOCEXtaGat1yTdoebYT0HP60:RrFfPjtmZzYfZlZuhBco1yTdosYT0H
Trid	43.5,UPX compressed Win32 Executable,42.7,Win32 EXE Yoda's Crypter,7.2,Win32 Executable (generic),3.2,Generic Win/DOS Executable,3.2,DOS Executable Generic

📁 File Paths ⌄

FILE PATH ON CLIENT	SEEN COUNT
C:\Users\mohit\Downloads\Compressed\DC Unlocker Cracked Version\dccrap.exe	1

⛓ PE Sections ⌄

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
UPX0	0x1000	0x982000	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
UPX1	0x983000	0x2e0000	0x2dfc00	7.94410943881	8baefd661d4a560925c2de56dfe4c36f
.rsrc	0xc63000	0x4000	0x3a00	3.64330998572	1e3ac3e9bf33922296832323144b983b