VALKYRIE

MALWARE
Valkyrie Final Verdict

File Name: Xenos.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 210a660c735cc5edf50a144955f5603820d4d680
MD5: 77a1cfe40b554d1c3bdfa36a5f1d347f
First Seen Date: 2018-12-21 00:59:53 UTC
Number of Clients Seen: 7
Last Analysis Date: 2019-01-25 20:21:39 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	2019-01-25 20:21:30 UTC	Malware
Static Analysis Overall Verdict	2019-01-25 20:21:39 UTC	No Threat Found
Precise Detectors Overall Verdict	2019-01-25 20:21:39 UTC	No Match
File Certificate Validation		Certificate and Vendor name are Not Valid

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	Suspicious
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	
Opens a file in a system directory	!

Behavioral Information

LoadLibrary

api-ms-win-core-synch-l1-2-0
kernel32
api-ms-win-core-fibers-l1-1-1
advapi32
api-ms-win-core-localization-l1-2-1
api-ms-win-security-systemfunctions-l1-1-0
api-ms-win-core-sysinfo-l1-2-1
comctl32.dll
UxTheme.dll
IMM32.dll
C:\Windows\system32\ole32.dll
C:\Windows\syswow64\MSCTF.dll
ADVAPI32.dll
OLEAUT32.DLL

ReadFile

C:\Windows\Fonts\staticcache.dat

OpenMutex

Local\MSCTF.Asm.MutexDefault1

WriteFile

C:\BlackBoneDrv7.sys

QueryFilePath

C:\Xenos.exe
C:\Windows\syswow64\MSCTF.dll
C:\Windows\syswow64\USER32.dll

OpenRegistryKey

\REGISTRY\MACHINE\SOFTWARE\M
\REGISTRY\MACHINE\SOFTWARE\Microsoft

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT	REASON
Static Precise PUA Detector 1	2019-01-25 20:21:35 UTC	No Match	NotDetected
Static Precise Trojan Detector 5	2019-01-25 20:21:35 UTC	No Match	NotDetected
Static Precise Trojan Detector 7	2019-01-25 20:21:35 UTC	No Match	NotDetected
Static Precise PUA Detector 4	2019-01-25 20:21:35 UTC	No Match	NotDetected
Static Precise PUA Detector 5	2019-01-25 20:21:35 UTC	No Match	NotDetected
Static Precise Trojan Detector 1	2019-01-25 20:21:35 UTC	No Match	NotDetected
Static Precise Trojan Detector 2	2019-01-25 20:21:35 UTC	No Match	NotDetected
Static Precise Trojan Detector 3	2019-01-25 20:21:35 UTC	No Match	NotDetected
Static Precise Trojan Detector 12	2019-01-25 20:21:35 UTC	No Match	NotDetected
Static Precise Trojan Detector 10	2019-01-25 20:21:35 UTC	No Match	NotDetected
Static Precise Virus Detector 1	2019-01-25 20:21:35 UTC	No Match	NotDetected
Static Precise Virus Detector 2	2019-01-25 20:21:35 UTC	No Match	NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Additional File Information

Vendor Validation - Not Verified ✖

[+] BlackBoneSPC

Status	Not Valid ✖

Certificate Validation - UntrustedRoot ✖

[+] BlackBoneSPC

Status	UntrustedRoot ✖
Start Date	2014-09-12 13:21:02
End Date	2040-01-01 01:59:59
Sha256	93dc090748281f1fab7be36d0ac60c6d5e9280da876fba931b73306ac72f5b41
Serial	E91647448FF1E7A84D4F7F62C30EAECB
Subject Name	BlackBoneSPC
Subject Key Identifier	null
Issuer Name	BlackBoneSPC
Issuer Key Identifier	bf a7 bb 91 b3 c7 fc 63 a6 8a 68 5a d3 cd 2f 7d
Crl link	null
Key Usage	null
Extended Usage	null

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x55D476EA [Wed Aug 19 12:30:34 2015 UTC]
Debug Artifacts	[object Object]
Entry Point	0x452638 (.text)
Exifinfo	[object Object]
File Size	1062720
File Type Enum	6
Imphash	a6f15c9b34b7bb1eedd081aeb95556fa
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Legal Copyright	Copyright (C) 2015
Internal Name	Xenos.exe
File Version	2.2.0.0
Product Name	Xenos
Product Version	2.2.0.0
File Description	PE injector
Original Filename	Xenos.exe
Translation	0x0400 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	5
Sha256	d69910f97bb6a19032297626a0cf1db5db56d00a4816791dc5e95e3e02587c4c
Ssdeep	24576:F/BzqvFlhdjg1WEL+8Vlsr9tPi+Ny4J0gbfysES9DsKRzoome/sBiBJeBIi:PmvFlhdjsNL++q9tc00gyvSZzZ1g
Trid	56.1,Win64 Executable (generic),26.6,Windows screen saver,9.1,Win32 Executable (generic),4,Generic Win/DOS Executable,4,DOS Executable Generic

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x8c4fb	0x8c600	6.61638414623	19745ee238f59d04e495ca29592ddaa3
.rdata	0x8e000	0x25888	0x25a00	4.48439894059	edc977bd714d6dceda7372f43194565f
.data	0xb4000	0x4228	0x2e00	4.4712743701	435459a2f044f7c75a29b83354b9247f
.tls	0xb9000	0x9	0x200	0.0203931352361	1f354d76203061bfdd5a53dae48d5435
.rsrc	0xba000	0x4dd20	0x4de00	6.14424169249	8d2c1f5ad0e95f2caca2647b3925c67d