VALKYRIE

MALWARE
Valkyrie Final Verdict

File Name: universal-extractor_3411208264.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: f2266f7628ab338d7c7d0fe143334e67d815d729
MD5: 120a04b01b5e9fc604a9b825d4c7b32e
First Seen Date: 2018-05-12 21:50:22 UTC
Number of Clients Seen: 7
Last Analysis Date: 2018-05-18 06:12:47 UTC
Human Expert Analysis Date: 2018-05-13 18:57:04 UTC
Human Expert Analysis Result: Malware
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2018-05-18 06:12:47 UTC	Malware
Static Analysis Overall Verdict	2018-05-18 06:12:47 UTC	No Threat Found
Precise Detectors Overall Verdict	2018-05-18 06:12:47 UTC	No Match
Human Expert Analysis Overall Verdict	2018-05-13 18:57:04 UTC	Malware
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	Clean
Timestamp value suspicious	Suspicious
Header Checksum is zero!	Suspicious
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	Suspicious
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

C:\Windows\system32\ole32.dll
C:\Windows\syswow64\MSCTF.dll
uxtheme.dll
shell32.dll
ADVAPI32.dll
ole32.dll
comctl32.dll
C:\Users\win7\AppData\Local\Temp\is-NDH2G.tmp_isetup_shfoldr.dll
shfolder.dll
Rstrtmgr.dll
C:\Windows\SysWOW64\bcryptprimitives.dll
UxTheme.dll
IMM32.dll
C:\Windows\system32\imageres.dll
C:\Windows\system32\shell32.dll
C:\Windows\system32\shlwapi.dll
OLEAUT32.DLL

ReadFile

C:\universal-extractor_3411208264.exe
C:\Windows\Fonts\staticcache.dat

OpenMutex

Local\MSCTF.Asm.MutexDefault1
DefaultTabtip-MainUI

WriteFile

C:\Users\win7\AppData\Local\Temp\is-NDH2G.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-NDH2G.tmp_isetup_setup64.tmp

CreateMutex

Local\RstrMgr3887CAB8-533F-4C85-B0DC-3E5639F8D511
Local\RstrMgr-3887CAB8-533F-4C85-B0DC-3E5639F8D511-Session0000
<NULL>

QueryFilePath

C:\Users\win7\AppData\Local\Temp\is-AQSVA.tmp\universal-extractor_3411208264.tmp
C:\Windows\syswow64\MSCTF.dll
C:\Windows\syswow64\USER32.dll

OpenRegistryKey

\REGISTRY\MACHINE\SOFTWARE\M
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control
\REGISTRY\MACHINE\SOFTWARE\Microsoft

CreateRegistryKey

\REGISTRY\US

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Static Precise PUA Detector 1	2018-05-18 06:12:44 UTC	No Match		NotDetected
Static Precise Trojan Detector 5	2018-05-18 06:12:44 UTC	No Match		NotDetected
Static Precise Trojan Detector 7	2018-05-18 06:12:44 UTC	No Match		NotDetected
Static Precise PUA Detector 4	2018-05-18 06:12:44 UTC	No Match		NotDetected
Static Precise PUA Detector 5	2018-05-18 06:12:44 UTC	No Match		NotDetected
Static Precise Trojan Detector 1	2018-05-18 06:12:44 UTC	No Match		NotDetected
Static Precise Trojan Detector 2	2018-05-18 06:12:44 UTC	No Match		NotDetected
Static Precise Trojan Detector 3	2018-05-18 06:12:44 UTC	No Match		NotDetected
Static Precise Trojan Detector 12	2018-05-18 06:12:44 UTC	No Match		NotDetected
Static Precise Trojan Detector 10	2018-05-18 06:12:44 UTC	No Match		NotDetected
Static Precise Virus Detector 1	2018-05-18 06:12:44 UTC	No Match		NotDetected
Static Precise Virus Detector 2	2018-05-18 06:12:44 UTC	No Match		NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2018-05-13 15:58:37 UTC
Analysis End Date: 2018-05-13 18:57:04 UTC
File Upload Date: 2018-05-13 07:20:49 UTC
Human Expert Analyst Feedback:
Verdict: Malware
Malware Family:
Malware Type: 0

Additional File Information

Vendor Validation - Not Verified ✖

[+] Innova Media d.o.o.

Status	Not Valid ✖

Certificate Validation - Success ✔

[+] Innova Media d.o.o.

Status	NoError ✔
Start Date	2017-10-03 03:00:00
End Date	2018-10-04 02:59:59
Sha256	03c257692ee85bfe36809a133833dd95f7aece457323d3d7b0665bc9e022b92d
Serial	6BA9602D09708A88C7F10AEF344D6D10
Subject Name	Innova Media d.o.o.
Subject Key Identifier	f6 b7 8b 9d 0a 53 cc 40 e9 86 16 81 42 7b e5 8c 63 a5 f2 51
Subject Organization	Innova Media d.o.o.
Subject Locality	Sempeter pri Gorici
Subject Country	SI
Subject Organizational Unit	IT
Issuer Name	thawte SHA256 Code Signing CA
Issuer Key Identifier	57 86 9b 54 b8 be a6 29 8a e4 f6 c2 e2 13 18 89 85 cd dc b7
Issuer Organization	thawte, Inc.
Issuer Country	US
Crl link	http://tl.symcb.com/tl.crl
Key Usage	Digital Signature (80)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

[+] thawte SHA256 Code Signing CA

Status	NoError ✔
Start Date	2013-12-10 02:00:00
End Date	2023-12-10 01:59:59
Sha256	d542ad03871f39ed7a47a057892a67f6d76b973134a8a129d2ba1ace821de2e4
Serial	71A0B73695DDB1AFC23B2B9A18EE54CB
Subject Name	thawte SHA256 Code Signing CA
Subject Key Identifier	57 86 9b 54 b8 be a6 29 8a e4 f6 c2 e2 13 18 89 85 cd dc b7
Subject Organization	thawte, Inc.
Subject Country	US
Issuer Name	thawte Primary Root CA
Issuer Key Identifier	7b 5b 45 cf af ce cb 7a fd 31 92 1a 6a b6 f3 46 eb 57 48 50
Issuer Organization	thawte, Inc.
Issuer Country	US
Issuer Organizational Unit	(c) 2006 thawte, Inc. - For authorized use only
Crl link	http://t1.symcb.com/ThawtePCA.crl
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	Client Authentication (1.3.6.1.5.5.7.3.2)

[+] thawte Primary Root CA

Status	NoError ✔
Start Date	2006-11-17 02:00:00
End Date	2036-07-17 02:59:59
Sha256	d6a37f73bd37d7adacb96997064639215d4806b63a4ccee5416e3da8d68a3b1f
Serial	344ED55720D5EDEC49F42FCE37DB2B6D
Subject Name	thawte Primary Root CA
Subject Key Identifier	7b 5b 45 cf af ce cb 7a fd 31 92 1a 6a b6 f3 46 eb 57 48 50
Subject Organization	thawte, Inc.
Subject Country	US
Subject Organizational Unit	(c) 2006 thawte, Inc. - For authorized use only
Issuer Name	thawte Primary Root CA
Issuer Key Identifier	undefined
Issuer Organization	thawte, Inc.
Issuer Country	US
Issuer Organizational Unit	(c) 2006 thawte, Inc. - For authorized use only
Crl link	undefined
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	undefined

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC] [SUSPICIOUS]
Debug Artifacts	
Entry Point	0x409c40 (CODE)
Exifinfo	[object Object]
File Size	2296648
File Type Enum	6
Imphash	884310b1928934402ea6fec1dbd3cf5e
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	3
Legal Copyright	
File Version	
Company Name	
Comments	This installation was built with Inno Setup.
Product Name	Kib
Product Version	1.2
File Description	Kib Setup
Translation	0x0000 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	8
Sha256	b7ff258576555f8ed08ed7bdf1481a068fc943f331d36b27125c81dea63e06a0
Ssdeep	49152:5fpFXSZ2G9f2RZSMaOBP5teehS0SzUFR5Z0YQhZIV4dyV3:5hte1OTd1Xew7ZiIB
Trid	45.2,Win32 Executable Delphi generic,20.9,Win32 Dynamic Link Library (generic),14.3,Win32 Executable (generic),6.6,Win16/32 Executable Delphi generic,6.3,Generic Win/DOS Executable

File Paths

FILE PATH ON CLIENT	SEEN COUNT
universal-extractor_3411208264.exe	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
CODE	0x1000	0x9364	0x9400	6.61113546404	ca8938e5c06d0356e32ba050b47e48ec
DATA	0xb000	0x24c	0x400	2.73730656229	5d98c64569668b0235ae89005918165a
BSS	0xc000	0xe88	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.idata	0xd000	0x950	0xa00	4.4307330698	bb5485bf968b970e5ea81292af2acdba
.tls	0xe000	0x8	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rdata	0xf000	0x18	0x200	0.20448815744	9ba824905bf9c7922b6fc87a38b74366
.reloc	0x10000	0x8b4	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rsrc	0x11000	0x2c00	0x2c00	4.4934749506	1d34d222f0ea847e102bf43f530ada66